6 Log Management Products p. 23 ■ Paul Thurrott on Windows Server 2008 p. 14

MANAGEMENT • SECURITY • NETWORKING • MESSAGING • HOW-TO

Windows® IT Pro

We're in IT with You

THE 4 PILLARS OF SYSTEM CENTER CONFIGURATION MANAGER p. 30

SCCM

Security Template Ah-has and Uh-ohs p. 45

Vista Deployment: Is WDS the Answer? p.40

REQUIRED READING

Get Exchange 2007 Ready to Run p. 55

Dig Into PowerShell p. 49

SHAREPOINT AND OFFICE PRO

SharePoint vs. Public Folders p. 61

Penton
A PENTON PUBLICATION
JULY 2007
WWW.WINDOWSITPRO.COM
U.S. $5.95 CANADA $7.95


VoIP AS YOU ARE.
VoIP AS YOU ARE.
VoIP AS YOU ARE.
VoIP AS YOU ARE.
VoIP AS YOU ARE.
VoIP AS YOU ARE.
VoIP AS YOU ARE.
VoIP AS YOU ARE.

Let's leave the hardware where it is.

Introducing the software-based VoIP solution from Microsoft. It's a whole new way to look at telephony.

As it turns out, that important move to VoIP isn't about ripping and replacing or big, upfront costs. That's because it's no longer about hardware.

It's actually about software.

That's right. Keep your hardware—your PBX, your gateways, even your phones. Add software. Software that integrates with Active Directory,® Microsoft® Office, Microsoft Exchange Server, and your PBX. Simply maximize your current PBX investment and make it part of your new software-based VoIP solution.

Because what you have is good. What you have with the right software is even better. Learn more at microsoft.com/voip

Your potential. Our passion.™

Microsoft®

Windows IT Pro
JULY 2007 VOLUME 13 NO. 7

COVER STORY

FEATURES

FEATURES

SHAREPOINT & OFFICE PRO

TRICKS & TRAPS

49

COLUMNS

"CorasWorks extends what you already know about SharePoint and builds on what you already have."

—Ronald Simmons, Director of knowledge management, US Marine Corps

PRODUCTS

WHAT'S HOT

IN EVERY ISSUE

Mark Minasi
Windows Power Tools
Chml Fills the Gap
In response to an Icacls shortcoming, Mark creates a free downloadable tool called Chml, which lets you further your integrity-level experiments.
InstantDoc ID 95973

Michael Otey
Top 10
Vista Customizations for Administrators
Make sure you've got Windows Vista organized so you can effectively perform your administrative functions.
InstantDoc ID 96011

Learning Path Article not a perfect fit? Find more resources to match your knowledge and skills.
Interact! Network with authors, peers, product vendors, and Microsoft.

Manage Any Data Center.
Anytime. Anywhere.

Avocent builds hardware and software to access, manage and control any IT asset in your data center, online or offline, keeping it, and your business, "always on".

Visit us on our Remote Control Tour. For locations near you, go to **www.avocent.com/remotecontrol.**

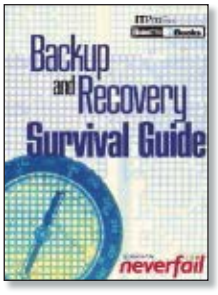
Avocent®
The Power of Being There®

Migrate Applications to a New OS

Take the necessary steps for migrating applications, from converting legacy applications to implementing MSI. Learn best practices—including Information Technology Infrastructure Library (ITIL) and Definite Software Library (DSL)—that are based on real-world examples of migrating applications to a new OS.

http://www.windowsitpro.com/go/seminars/macrovision/appmanagement/?code=julycitc

"Backup and Recovery Survival Guide"



You can't control what nature throws at your IT systems, like floods, hurricanes, and earthquakes. You can't always control what people might do to your systems, either. Download this free eBook and learn to protect your business in the face of a natural or human-made disaster.

http://www.windowsitpro.com/go/ebooks/neverfail/backup/?code=julycitc

"Build a World Class End-to-End Web Filtering Solution in 5 Steps"

IT departments spend time and energy creating and managing firewall rules and router tables yet overlook the direct channel between the Internet and computers on the corporate network. It takes just one user to cause problems by downloading a virus or viewing objectionable content. Learn how to build a world-class Web-filtering solution in five steps.

http://www.windowsitpro.com/go/podcast/stbernard/endtoend/?code=julycitc

Situation Room Blog: Experts and Resources When You Need Them

When Microsoft security fires flare, when a crucial patch affects your network's ability to function, when you need information about an event that could affect your network, our "IT 911" blog, Situation Room, is required reading. *Windows IT Pro* authors and editors give you the information you need and provide expert insight and real-world experiences to help you make the right decisions.

http://www.windowsitpro.com/blog

The Missing Link to IT Resources

So many IT products and services options are available that it's hard to keep them straight—let alone decide which is the best solution. This year, our editors have done that hard work for you. Coming in our August issue, the 2007 Editor's Best Awards announces the best solutions in interoperability, security, systems management, hardware, and more. Our editors chose the best products in their areas of expertise and interviewed users to help explain what makes the products so special. Here's a sneak peek of what's to come.

"Peace of mind is something IT pros want but don't often have—there's always something, somewhere, that can and will go wrong with your system. Among the huge number of systems management products that come across my desk, one solution stands out . . ."

—Caroline Marwitz, systems management

"The network-management marketplace is flooded with products that claim to help you better oversee your network infrastructure and environment. I talk to vendors around the world, and each one seems to offer a unique answer to that age-old IT administrator plea: How can your product make my life easier?"

—Jason Bovberg, network

2007 *Windows IT Pro* Innovators Contest: Open for Entries!

Have you developed a solution that uses Windows technology to solve a business problem in an innovative way? Enter your solution in the 2007 *Windows IT Pro* Innovators Contest! Top winners will receive great prizes and will be profiled in the November 2007 issue.

http://www.windowsitpro.com/awards/innovators_2007.cfm

LIEBERMANSOFTWARE

Are local Administrator accounts setting you up for a fall?

NEW!
VERSION 3.0

Sharing a common password across local Administrator accounts endangers your networked systems!

The convenience of using the same local administrator password on all your systems comes with a serious downside. If a user cracks the password on just one machine, he or she instantly gains peer-level access to your entire network. Manually setting, changing, tracking, and auditing these passwords is prohibitively difficult — but there is a solution. **NEW Random Password Manager 3.0** gives you the power to easily, dynamically, and automatically manage local administrator passwords. Stop the chain reaction before it starts. Get **Random Password Manager 3.0** today!

LEARN MORE!

1-800-829-6263
sales@liebsoft.com
(01) 310.550.8575

- Creates unique, cryptographically complex passwords across the enterprise.
- Retrieves passwords on demand through a secure web interface.
- Re-randomizes recovered passwords after a fixed period of time.
- Supports Windows, Unix, Linux, and SQL Server password randomization.
- Issues temporary administrator privileges to delegated users.
- Eliminates the need for Vista users to contact Help Desk when UAC requests administrator credentials.
- Sets up easily; scales from small to large environments with no agents needed.

DOWNLOAD A FREE EVAL! www.liebsoft.com/rpm

Microsoft GOLD CERTIFIED Partner

I Know Who You Are; I Saw What You Did

NAP protects your network from nasty things users pick up

"Don't put that in your mouth! You don't know where it's been!" You can't always prevent a child from trying to eat a piece of candy that has fallen on the floor. But you can reach out and grab the candy before it goes into the child's mouth. And despite your best intentions, children will sometimes manage to swallow something unsavory and end up sick, so you have to put them to bed and give them medicine until they're well. Like kids who are innocently oblivious to the dangers of unclean food, computer users attach their laptops and mobile devices to your network after taking them from the office and working with them on unsecured networks. It's enough to make you want to yell: "Don't let that on my network! I don't know where it's been!"

That unappetizing analogy came to me during a recent briefing on Microsoft's Network Access Protection (NAP) technology, which is part of Windows Server 2008 (formerly code-named Longhorn) and Windows Vista. If you have policies about what requirements make a machine safe to access your network, NAP gives you a way to enforce those policies and remediate non-compliant machines so that they can come back onto the network once they meet your policy requirements again. If a machine doesn't have the correct level of security patch or the latest antivirus definitions or doesn't meet your other policy requirements, NAP catches the machine before it accesses network assets and keeps the machine isolated until the problem has been fixed.

Early NAP Adopters

Microsoft's Mike Schutz told me that early adopters are already using NAP in industries such as education, financial services, and professional services. In education, for example, Mike said, "especially with lots of students coming back on campuses with their laptops, administrators want to be able to set policies so that these laptops come back on the network and don't infect it. One of our early beta customers is Louisiana State University—LSU—which has already deployed NAP across part of the campus and is currently enforcing NAP using DHCP. Even internally at Microsoft we have over 75,000 clients that are enforced using NAP at the Redmond campus and parts of Latin America and parts of EMEA [Europe, the Middle East, and Africa], all centrally managed in Redmond."

NAP and Interoperability

Education environments make perfect sense as early adopters of NAP, and Microsoft's recent announcements about NAP interoperability also seem relevant for universities, which tend to have a lot of non-Windows systems. And Microsoft's NAP solution is not the only player on this field. Microsoft's Henry Sanders (a Microsoft Distinguished Engineer and the general manager of the Core Networking and Collaboration group in Windows Networking), explained, "[T]here are three primary NAC architectures: Microsoft's NAP, the Trusted Computing Group's Trusted Network Connect (TNC), and Cisco's Network Admission Control, or C-NAC. In September, Microsoft announced an interoperability agreement with Cisco's NAC solution. At the [recent] Interop trade show, Microsoft announced that NAP would now be interoperable with the Trusted Computing Group's TNC. The TNC agreement makes NAP's Statement of Health (SoH) protocol, included in Windows Vista, the standard client-server communication protocol within TNC. We are very excited because, with this announcement, Microsoft's NAP is now interoperable with the two other primary NAC architecture solutions, TNC and Cisco's NAC."

Sanders continued, "[O]rganizations can now standardize on the (SoH) client protocol, regardless of their NAC infrastructure. The SoH client is available in Windows Vista, will be available in the next service pack of Windows XP, and through NAP partners for non-Microsoft operating systems. One of our NAP partners, Avenda Systems, is releasing a NAP client for the Linux operating system. The broad level of interoperability removes a major adoption barrier by providing investment protection, because organizations can deploy NAP into their existing infrastructure without having to rip and replace their existing investments."

Security: People *and* Machines

To keep your network secure, you need to know not only *who* is accessing your resources but also the health of their machines. NAP is designed to keep your network safe no matter where your users have taken their devices, but you need to do your part by devising the appropriate policy requirements that determine what NAP is looking for. As Mike put it, you have to know "what healthy means to you. That changes for each organization, so you have to define a security policy. That's not a statement about technology; it's people and processes. Then, you think about how to enforce that policy, and that's where NAP comes in."

InstantDoc ID 95523

Karen Forster (karen@windowsitpro.com) is editorial and strategy director for *Windows IT Pro* and *SQL Server Magazine* and former director of Windows Server User Assistance at Microsoft.

WRITING FOR *WINDOWS IT PRO*

Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.

PROGRAM CODE

SUBSCRIPTION INFORMATION

Subscriptions in US, $49.95 for one year (12 issues for 2007); in Canada, $59 US currency, plus 7% for GST for-one year; in UK £59; in all other countries, US $99. Payment should be made in US dollars drawn on US banks. For new subscriptions, call 800-793-5697 or 970-663-4700, or check our Web site at http://www.windowsitpro.com. For questions or other subscription problems, call customer service at 800-793-5697 or email subs@windowsitpro.com. Europe, europe@windowsitpro.com, *Windows IT Pro,* Di-An House, 2 Aegean Road, Atlantic Street, Altrincham, Cheshire, WA14 5UW, England; tel.-0161 929 2800, fax-0161 929 1511.

Your comprehensive must-have everyday solution, learn more today!

www.visualclick.com

Visual Click

Toll Free 877 902 5425
Direct 512 330 0542

Upgrade to Next-Generation Antispam/Antivirus for Exchange.

SUNBELT MESSAGING NINJA™ for Exchange

Osterman Research: "Half the admin time!"

SC MAGAZINE AWARDS 2007 WINNER Honored in the U.S.

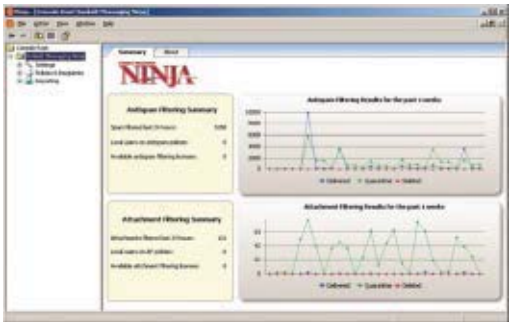
Windows IT Pro READERS CHOICE 2006 Winner

2006 Products of the Year SearchExchange.com

Meet Sunbelt Messaging Ninja: The award-winning all-in-one, best-of-breed, third-generation messaging security solution. Ninja is a plug-in framework that integrates best-of-breed antispam, antivirus, disclaimers and SMART attachment filtering on your Exchange server.

Half the admin time: Independent research shows that Ninja requires one-half the IT time to manage than other comparable email management systems.* With its MMC interface, Ninja is easy to manage so you can get up and running in minutes vs. hours.

Better multi-engine spam detection: Ninja's filtering decimates junk mail and image spam with both Cloudmark (which includes antiphishing) and Sunbelt's own heuristics-based iHateSpam engines. Of course, it also supports RBLs and SPF.



Integrated multi-engine antivirus: Ninja combines the power of multiple high-quality AV engines.

Great end-user control: The policy-based plug-in architecture allows you powerful, granular control. You can finally rule with an iron fist.

SMART attachment filtering: Ninja features the first flexible policy-based attachment filter that isn't fooled by extensions. It looks inside files to determine their true identity. Your policies decide what happens to all attachments.

Download your evaluation copy at:
www.sunbeltsoftware.com/ninjawinb

Sunbelt Software

Email sales@sunbeltsoftware.com or call 888-688-8457 for your 50% discount competitive upgrade quote

Sunbelt Software Tel: 1-888-688-8457 or 1-727-562-0101 Fax: 1-727-562-5199 www.sunbeltsoftware.com sales@sunbeltsoftware.com

The competitive upgrade is based on 50% of Ninja list price.

*Based on Osterman Research report "Comparing Email Management Systems that Protect Against Spam, Viruses, Malware and Phishing Attacks". December 2006.

VoIP: You Can, and Maybe You Should?

I read Mark Minasi's Web exclusive article "VoIP: Just Because You Can Doesn't Mean You Should" (InstantDoc ID 95980), and I think you're missing something important. If VoIP is such a Bad Thing, why is it that the wireline telephone companies are investing so heavily in it? Recall that the core of the Vonage lawsuit is a claim by Verizon that Vonage violated patents owned by Verizon. In my opinion, the wired-line telephone companies are milking their switched networks for all they're worth, while they prepare for the day when they're outdated, and must be dismantled.

Several things are leading in that direction. I suspect the one that is most likely to lead to the demise of the Public Switched Telephone Network is that we run out of telephone numbers, or must face the prospect of extending the area code, the exchange number (the middle digits), or the number itself (the last four digits). If you thought Y2K was bad, just think about the consequences of that sort of change.

—David Gray

I liked Mark Minasi's article, but I have Comcast phone service (which is VoIP) because I get unlimited long distance for a fraction of the wired-line price.

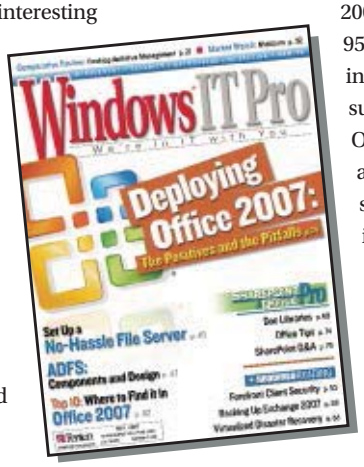
—Rich (last name withheld)

I switched to VoIP last year because the price was significantly less than the traditional telco that held a near monopoly, and I got many more features for free than the telco could offer even at extra cost. I deliberately avoided Vonage because of the pending lawsuit and waited more than a year until the level of reported dissatisfaction with service and call quality for the company I chose had stabilized and improved.

—Marcus Patz

IT's Unintended Impact on Productivity

Karen Forster's IT Pro Perspective: "Discovering the Midmarket Opportunity" (May 2007, InstantDoc ID 95669) was an interesting take on the idea that IT contributes positively to general productivity. My 20 years of experience in distance education indicates that IT is the second greatest contributor to lost man hours next to sick leave.



I can remember times when I would arrive at work in the morning to find the database down because the overnight refresh failed. There were times when this would happen every morning without fail for weeks on end. We would have to wait for the technician to arrive, and a couple of hours later the database would be back up. With more than 250 workstations affected, we lost something like 500 man hours every day, and some weeks as much as 2500 hours. This was all Microsoft software.

—Bernie Kemp

Kudos to Ben Smith

I just noticed that Ben Smith won't be presenting at TechEd this year. That's unfortunate. I quite enjoy reading Ben's "The Business End" articles about technical management. I think this is one of the most overlooked areas in the IT profession—and it's something that's near and dear to my heart. If he hasn't already thought about it, I hope Ben considers writing a book about managing a technical staff.

—Hunter French

Office 2007 Deployment Without Group Policy Is a Mistake

I read Dan Holme's "Customizing and Deploying Office 2007" (May 2007, InstantDoc ID 95433). It's disappointing that Microsoft won't support Group Policy for Office 2007 installations, and I can't believe Microsoft would reduce such important functionality in an upgrade like this. I have used Group Policy to deploy Office for years to small businesses that don't have Microsoft Systems Management Server (SMS) installed, and it has been a salient time-saver (clients are concerned about this when you're on the clock).

I think Microsoft should immediately rethink this errant policy and support Office 2007 installation via Group Policy. We hear so much from Microsoft about running as non-administrators or about user account control, but now you must install Office as an administrator. This doesn't make any sense and should be reversed because it will become an unpleasant surprise to many people when they attempt to deploy Office.

—W. O. Sully

Good on You, Eric Rux

Eric Rux's article "Let's Get Organized: File Server Basics" (May 2007, InstantDoc ID 95354) is excellent. Although Eric's recommendations seem to be the obvious way to configure a file server, you never see basic information like this presented so well. This is a real-world, practical article that I don't think we see enough of.

—Todd Lester

InstantDoc ID 95789

EDITOR'S NOTE

Windows IT Pro welcomes feedback about the magazine. Send comments to letters@windowsitpro.com, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.

_INFRASTRUCTURE LOG

_DAY 78: Our energy costs are staggering! We're spending more to power and cool the hardware than we did to buy it in the first place. We can't get enough power into our data center.

_It's too darn hot. Gil moved the entire data center to the Arctic Circle. This commute is ridiculous.

_DAY 81: I'm taking back control with IBM energy management solutions. IBM services helped us identify inefficiencies and change our entire approach to power and cooling. The IBM System z™ server's high utilization and unique design is très cool. We no longer have to feed the never-ending power appetite of our old, high-density environment. We've moved the data center back where it belongs.

_Gil doesn't want to hear about it. He says he's snow deaf.

IBM.COM/**TAKEBACKCONTROL**/EFFICIENCY

What You Need to Know About ...

Windows Server 2008 Beta 3

This is the big one

Paul Thurrott (thurrott@windowsitpro.com) is the news editor for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (http://www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (http://www.wininformant.com).

After many months of delays, Microsoft finally released the Beta 3 version of Windows Server 2008—previously code-named "Longhorn"—a major milestone prerelease version of the next version of Windows Server. Windows 2008 has evolved quite a bit over time, and though the project hasn't suffered from the many feature drops and problems that dogged Windows Vista, Beta 3 certainly has a few surprises. Here's what you need to know about Windows 2008 Beta 3.

The Basics

Windows 2008 will boast enhanced scripting and task automation via the new Windows PowerShell—a surprise addition to Beta 3, given that PowerShell was originally not going to ship as part of this product. In addition, Windows 2008 will have improved roles-based installation and management capabilities that extend to Windows Server Core, a new lightweight and safer version of the OS that provides only a subset of roles available in the mainstream server versions.

Like Windows Vista, Windows 2008 includes increased security prowess. The Windows Firewall is enabled now by default, for example, and in branch offices Windows 2008 can be installed using technologies such as Read Only Domain Controller (RODC) and BitLocker, which can help ensure that physical server theft won't result in a major security disaster. Windows 2008 also includes the long-awaited Network Access Protection (NAP) feature, which finally brings policy-based network quarantining to the Windows platform.

On the flexibility front, Windows 2008 adds some intriguing new Terminal Services improvements that will allow organizations to deploy remote environments and even remote applications, both within their firewall and beyond. And eventually, the inclusion of the Windows Server Virtualization piece (as an optional add-on) will provide Windows 2008 with a more performance-friendly and secure bare metal virtualization solution, though that piece isn't present in Beta 3.

Did You Know?

Paul provides an in-depth review of Windows Server 2008 Beta 3 at the SuperSite for Windows (http://www.winsupersite.com/reviews/lhs_beta3.asp).

Moving to Beta 3

In the gear-up to Windows 2008 Beta 3, Microsoft has made a number of improvements. Windows Firewall is configured to open and close only the required ports as roles and features are installed and removed, resulting in the most secure Windows Server version yet. Server Manager, Microsoft's central console for daily server administration tasks, has been improved and augmented by a new command-line tool called servermanagercmd.exe that provides administrators with all of Server Manager's functionality from the command line.

Speaking of command lines, the Server Core installation type has been augmented with a new command-line tool called oclist.exe, which provides a way to examine the roles and features that are installed in the Server Core environment. Microsoft has also increased the number of roles with the addition of new Active Directory Lightweight Directory Services (AD LDS), Print, and Windows Media Services (WMS) roles. (Other roles, such as Web Server and Virtualization, will be made available later.) The seven roles available in Beta 3 include AD, AD LDS, DNS, DHCP, WMS, File, and Print.

Beta 3 itself includes some Terminal Services improvements over past versions of Longhorn. A new feature called Easy Print makes it, well, *easy* to print from a Terminal Services-based environment or application to your default printer. Remote Programs has been rebranded as Terminal Services RemoteApp. You can seamlessly copy and paste between a Terminal Server session and the host OS, which is a huge improvement. And Terminal Services now supports 32-bit color sessions, increased from 24-bit in previous versions.

NAP has been updated so that you can remediate connecting clients via Windows Update or Microsoft Update if your local Windows Server Update Services (WSUS) box is unavailable. You can now integrate NAP with Cisco's Network Admission Control (NAC) quarantine solution as well, which was the ostensible reason for delaying NAP's release from Windows Server 2003 R2 to Windows 2008. And a new, simple, wizard-based UI makes setting up and managing NAP easier than ever.

Drilling Down

Looking over the long list of new and improved Windows 2008 features, a number of them stand out. The new Server Manager is turning into a true one-stop shop for an admin's daily management needs. Here, you'll see nodes in the Microsoft Management Console (MMC) UI for all of the installed roles and features; troubleshooting tools such as the new XML-based Event Viewer and the new Vista-like reliability and performance tools; configuration tools such as Task Scheduler, Windows Firewall, Windows Management Instrumentation (WMI) Control, and Device Manager; and storage and backup tools such as Windows Server Backup (finally, a replacement for the miserable NTBackup) and Disk Management, which can resize NTFS-based volumes on the fly.

Server Manager is the culmination of years of work in management UIs. In the topmost "home page," you'll see a variety of information about the server that's currently connected, along with task pads for editing server configuration information. Other commonly needed server attributes (e.g., security, roles, features) are also available from this home page, which isn't a dashboard, but rather an interactive cockpit. That is, you can view installed features, for example, but you can also install and uninstall features from this home page and drill deeper into the functionality of installed features.

Server Core is one of the most intriguing things about Windows 2008. This stripped down installation type lets you configure a GUI-less, headless server with one to seven roles, including AD, AD LDS, DNS, DHCP, WMS, File, and Print (and it will eventually include Web Server and Windows Server Virtualization). Server Core opens into a blank desktop and a single command-line window. There's no shell, Microsoft Internet Explorer (IE) browser, Windows Media Player, or any other pointless graphical application.

The point behind Server Core is to provide only core server features and to do so in the most secure way. Because of the roles-based installation and management aspects of Windows 2008, each of the Server Core roles are installed in a manner that significantly reduces the attack surface of the server. Note that Server Core-based servers are still based on Windows 2008, and thus provide the same connection capabilities: You can still manage them remotely using the GUI-based tools you already know and love, from another server or a desktop machine.

Windows 2008, like Vista, includes the useful BitLocker utility, which I covered in "What you need to know about Vista's User Account Control and BitLocker Drive Encryption" (April 2007, InstantDoc ID 95153). BitLocker provides full volume disk encryption for all disks attached to the server; this is a new feature: In Vista, only the system disk was protected by default. BitLocker is even more useful when used in tandem with other Windows 2008 technologies. For example, businesses looking for the most secure and easily managed branch office servers could install BitLocker alongside Server Core and RODC for the most secure configuration possible. If the server is stolen, no data can be taken and hackers won't be able to access the passwords for all domain users since only the passwords for the locally cached users—and not the administrators—are stored locally on the box.

On the Terminal Services front, a new mode called Terminal Services Gateway tunnels remote sessions through HTTP Secure (HTTPS) so that you don't need to configure a VPN, but can still access Terminal Services from wireless locations that specifically block VPNs. Remote sessions connected in this fashion are marked with the same "secure lock" graphic that users are familiar with from IE 7.0. Terminal Services RemoteApp delivers individual applications, instead of separate remote sessions, to users' desktops. After users log on, the effect is seamless and almost identical to running the application locally.

Windows Server 2008's new Server Manager is turning into a true one-stop shop for an admin's daily management needs.

What's Missing?

As I made reference to earlier, one of the most eagerly awaited Windows 2008 technologies—Windows Server Virtualization, codenamed "Viridian"—is missing in Windows 2008 Beta 3. Indeed, in the weeks before shipping Beta 3, Microsoft warned that it would not be able to ship a public beta of Viridian until the second half of 2007. The revolutionary technology was previously expected in the first half of the year; however, Microsoft still claims that it will be able to ship Windows Server Virtualization within 180 days of the release of Windows 2008. The company plans to make this technology available separately from Windows 2008, as a free update. Whenever it is released, Windows Server Virtualization will be made available as a new server role in both Server Core and the mainstream installations of Windows 2008. Sadly, even that version of Virtualization will be scaled back from Microsoft's original promises: The company recently announced that it will no longer include three critical features: live migration support; the ability to hot-add storage, networking hardware, memory, and processors; and support for up to 32 processor cores (the initial version of Virtualization will support just 16 processor cores).

Another significant omission is that Windows 2008 Beta 3 doesn't support a Web server or application server role in Server Core. The issue is the Microsoft .NET Framework, which would be required in either scenario for either role. Current versions of the .NET Framework include a variety of GUI-based libraries, which wouldn't work properly in Server Core. Microsoft is investigating whether to create a Server Core-friendly .NET Framework subset for a future release. But I've been told that, post-Beta 3, the company will add a new Web Server role to Server Core that includes all Microsoft IIS 7.0 functionality except for ASP.NET, which does require .NET. This solution will give Microsoft an effective answer to low-end Linux/Apache Web servers.

One potential problem with Windows 2008 is its dual nature. Although the roles-based management approach means the system will always configure settings correctly when you use the GUI tools, it's still possible to go into other tools, change settings, and end up configuring options incorrectly. Consider Windows Firewall as a likely scenario: When you install or configure a role such as Application Server, the firewall is automatically configured so that the role will function correctly. But you can still go into the Windows Firewall GUI and manually override those settings. There's no "secure for currently configured roles" fallback switch.

Recommendations

Microsoft says it is on track to deliver Windows 2008 by the end of 2007 and Windows Server Virtualization by late 2007 or early 2008. Those dates might be a bit optimistic if the number of unexpected Beta 3 delays is any indication, but no matter. Windows 2008 is on the way, and it's time for businesses of all sizes to begin evaluating this next-generation Windows Server version. Beta 3 is near-feature-complete and will be widely available by the time you read this, so now is the time to begin your evaluation. Windows 2008's feature set is so vast, as are the installation possibilities, that you'll want to take the time to really understand how this release will affect your environment.

InstantDoc ID 96068

EDITOR'S NOTE

Share your Windows discoveries, comments, solutions to problems, and experiences with products and reach out to other *Windows IT Pro* readers (including Microsoft). Email your contributions to r2r@windowsitpro.com. Please include your phone number. We edit submissions for style, grammar, and length. If we print your submission, you'll get $100. Submissions and listings are available online at http://www.windowsitpro.com. Enter the InstantDoc ID number in the InstantDoc ID text box.

Change IP Settings in a Snap

After spending a frustrating evening manually changing the IP settings for my Ethernet and wireless network adapters numerous times, I decided to create a tool that would automatically change IP settings. I wanted it to

- be a command-line tool
- have easily remembered syntax
- make default assumptions
- allow me to change all the IP settings at once
- allow me to change the IP settings for any card in my system
- have integrated Help and version information

The result is SetIP.cmd. This script lets you quickly and easily change the IP address, subnet mask, gateway, and DNS server for Ethernet and wireless network adapters. When you have more than one adapter of a type (e.g., two Ethernet network adapters, two wireless network adapters) the script will display the adapters one by one and let you select the one you want to configure. I've used SetIP.cmd with various versions of Windows XP. It should work fine with Windows 2000, but I haven't done much testing in that environment. Initial reports indicate possible problems with using it on server OSs, such as Windows Server 2003. (I wrote this script for use on client OSs.)

SetIP.cmd uses the Netsh Interface IP commands to change IP settings. Although these commands are useful, their syntax is complicated and difficult to remember. So, SetIP.cmd generates the Netsh Interface IP commands for you. You just need to provide basic information on the command line using syntax that's much easier to remember.

SetIP.cmd uses the following defaults, unless you specify otherwise on the command line:

- It sets the IP settings for an Ethernet network adapter.
- It sets the IP address to 192.168.1.2.
- It sets the subnet mask to 255.255.255.0.
- It sets the gateway to *netAddress*.1, where *netAddress* is the first three octets of the IP address in a 24-bit subnet (i.e., 192.168.1.1 with the default IP address).
- It sets the DNS server to 4.2.2.2.

You can change the Ethernet network adapter, IP address, subnet mask, gateway, and DNS defaults by modifying the :PREP section, which Listing 1 shows. (You can download the entire script from the *Windows IT Pro* Web site.)

To launch SetIP.cmd, you follow the syntax

```
Setip [dhcp | <IPAddr>]
  [mask <SubnetMask>]
  [gw <DefaultGateway>]
  [dns <DnsServerAddr>]
  /w /nodns
```

If you launch the script with no parameters, all the default values just specified are set. When you want the DHCP server to select the IP address, you specify dhcp. When you want a static IP address, you specify that IP address.

The script has three other optional parameters: mask, gw, and dns. You use the mask parameter when you want to change the subnet mask to a value other than the default. The gw parameter lets you set the gateway to a value other than the default. You use the dns parameter to set the DNS server to a value other than the default.

The script also has two optional switches: /w and /nodns, which are case-sensitive. If you're configuring a wireless network adapter rather than an Ethernet network adapter, you include the /w switch. You use the /nodns switch if you want to skip configuring the DNS server setting. (During testing, I often just need to check network connectivity and therefore don't want Netsh to configure the DNS server setting.)

Let's look at some examples. Suppose you want to set an Ethernet network adapter's IP address to 192.168.1.2, subnet mask to 255.255.255.0, gateway to 192.168.1.1, and DNS server to 4.2.2.2. Because the address, subnet mask, gateway, and DNS server settings are the defaults, you just need to run the command

```
Setip
```

If you want to set a wireless network adapter's IP address to 10.20.30.5 and set its subnet mask, gateway, and DNS server settings to the defaults (255.255.255.0, 10.20.30.1, and 4.2.2.2, respectively), you'd use the command

```
Setip 10.20.30.5 /w
```

If you want to set an Ethernet network adapter's IP address to 192.168.2.9, subnet mask to 255.255.255.128, gateway to 192.168.2.2, and DNS server to 192.168.2.12, you'd run the command

```
Setip 192.168.2.9
  mask 255.255.255.128
  gw 192.168.2.2
  dns 192.168.2.12
```

If you want the DHCP server to automatically set all the IP settings, you'd use the command

```
Setip dhcp
```

Because I frequently use SetIP.cmd to check network connectivity, I often first set the Ethernet network adapter to a static IP address, then change

Listing 1: The :PREP Section from SetIP.cmd

```
:PREP
  Setlocal
  Set NicType=Local
  Set doDNS=Yes
  Set ipAddr=192.168.1.2
  Set ipMask=255.255.255.0
  Set dns=4.2.2.2
  Set ipType=static
  If Not {%1}=={} Set ipAddr=%1 & Shift
  If "%ipAddr: -1,1%"=="" " Set ipAddr=%ipAddr: 0,-1%
  If "%ipAddr%"=="mask" Set ipMask=%2 & Set ipAddr=192.168.1.2
  If "%ipAddr%"=="gw" Set ipGw=%2 & Set ipAddr=192.168.1.2
  If "%ipAddr%"=="/w" Set NicType=Wireless & Set ipAddr=192.168.1.2
  If "%ipAddr%"=="-w" Set NicType=Wireless & Set ipAddr=192.168.1.2
  If "%ipAddr%"=="/nodns" Set doDNS= & Set ipAddr=192.168.1.2
  If "%ipAddr%"=="-nodns" Set doDNS= & Set ipAddr=192.168.1.2
  If "%ipAddr%"=="dhcp" Set ipType=source=dhcp & Set ipAddr= &
     Set dns= & Set ipMask=
  If "%ipType%"=="static" Set metric=1 & Set register=none
  Goto GetCmdLine
```

it back to an IP address generated by the DHCP server, ignoring the DNS server setting in both instances. In this scenario, the commands look like

```
Setip 10.1.1.2 gw 10.1.1.254 /nodns
Setip dhcp /nodns
```

SetIP.cmd evolved out of my personal testing in various environments and has served me well. I hope you find it equally as useful.

—Matthew C. Miller, CTO, Stability Networks

InstantDoc ID 96113

Allow Cookies but Not Other Web Site Content

At my workplace, users regularly visit some Web sites in which they have to register. These sites require users to enable cookies in Microsoft Internet Explorer (IE) so that they can sign in. However, we use Group Policy, and our domain's default policy disables all cookies.

Because cookies from Web sites in IE's *Local intranet* and *Trusted sites* zones are accepted, you can typically enable cookies for certain Web sites by using Group Policy to add those sites to one of those zones. But what if you want to allow cookies but not all the other content that goes along with trusting a site? For example, you might want users to be able to log on to a site that requires registration (and therefore allow cookies), but you don't want users to be able to download files or install ActiveX objects from the site. This was the case at my company.

Because adding Web sites to the *Local intranet* or *Trusted sites* zone wasn't an option, I looked into whether I could use a Group Policy setting to centrally define exceptions for cookies. I was unable to find such a setting.

Not wanting to have to teach each user how to define exceptions in IE, I decided to come up with my own solution. I used RegMon (http://www.microsoft.com/technet/sysinternals/utilities/regmon.mspx) to track where IE stores cookie settings. I found that the settings are under the HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P\History registry key.

To accept cookies from a domain, I created a new subkey and gave it a default DWORD value of 1. For example, to accept cookies from the microsoft.com domain, I created the HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P\History\microsoft.com subkey and gave it a default DWORD value of 1.

Apostolos Fotakelis

You can't use regedit to create a subkey with a default DWORD. (When you create a subkey, regedit automatically creates a default REG_SZ value.) So, I used .reg files to create the subkeys. For example, Figure 1 shows the .reg file for creating the microsoft.com subkey.

I then wrote a batch file that uses the reg.exe utility to read and apply the .reg files. (Reg.exe is built into Windows Server 2003 and is part of the Windows 2000 Support Tools.) I inserted the batch file in a Group Policy Object (GPO) under User Configuration\Window Settings\Script\Logon Scripts.

With this solution, I can allow cookies but prevent users from downloading unwanted and possibly malicious files and ActiveX objects. Because the solution uses Group Policy, it's easy and quick to implement.

—Apostolos Fotakelis

InstantDoc ID 96114

Another Way to Ensure Automatic Shutdowns

In the Reader to Reader article "Flawless Automatic Shutdown of Client Computers" (November 2006, InstantDoc ID 93262), Milos Puchta described a problem he was having with a batch file that was supposed to shut down Windows XP Professional machines running ALWIL Software's Avast! antivirus software. This software prevents users from logging off when there's a disk (e.g., CD-ROMs, USB flash disks) in one of the computer's removable disk drives. Milos discovered that sometimes users left for the day, leaving disks in those drives. As a result, the shutdown process failed and the computers were left on all night.

Milos solved the problem by using the Shutdown command in a batch file. Another solution is to use PsShutdown, a free command-line utility (http://www.microsoft.com/technet/sysinternals/utilities/psshutdown.mspx). You can configure each PC with the PsShutdown utility (copied locally through a logon script if needed) and use a scheduled job with the appropriate command-line switches. You can create a job file on one PC, then copy it to the other PCs. If you don't need to shut down a particular PC, you can delete the job file by using a logon script. PsShutdown doesn't require the computer's name (it assumes the local PC), so using this utility would save Milos time because he wouldn't have to configure batch files.

For remote machines, you can copy PsShutdown and the job file by using commands such as

```
Copy shutdown.job
  \\labpc01\c$\windows\tasks
Copy psshutdown.exe
  \\labpc01\c$\windows\
```

To run these commands, you need administrative rights on the lab PC and there can't be any local firewalls.

Alternatively, Milos can schedule a job or use a Group Policy shutdown script to shut down the Avast! service prior to shutting down the XP Pro computers. (This is assuming you can't configure Avast! to ignore CD-ROMs or USB flash disks on shutdown.) Once again, this can be done remotely if needed. By shutting down the right service, it should stop the problem of machines not shutting down because CD-ROMs or USB flash disks were left in PCs.

—Edward Braiter

InstantDoc ID 96115

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P\History\microsoft.com]
@=dword:00000001
```

Figure 1: The .reg file for creating the microsoft.com subkey

Blake Eno (products@windowsitpro.com) is product editor for *Windows IT Pro* and *SQL Server Magazine.*

Product Spotlight

Networking Infrastructure

Increase Server Utilization

Alacritech's Scalable Network Accelerators (SNAs) and iSCSI Scalable Network Accelerators (iSNAs) offload TCP processing from Windows Server 2003 and Windows Storage Server 2003, letting those systems use their resources for application rather than network processing. Alacritech's accelerators allow network servers to support more users and storage and improve application performance. The new SNA and iSNA products support Microsoft TCP Chimney Offload technology, which helps optimize server performance. TCP Chimney Offload is part of the Windows Server 2003 Scalable Networking Pack.

Alacritech has introduced six SNA products—three for the workstation market (the SENI500 series) and three for the volume server segment (the SENI800 series)—plus three new iSNA products (the SESI800 series). You can evaluate Alacritech's products by visiting the Alacritech Product Evaluation eStore at http://shopping.netsuite.com/s.nl/c.ACCTI36534/sc.I/.f. For more information, contact Alacritech at 408-287-9997 or 877-338-7542 or visit Alacritech's Web site at http://www.alacritech.com.

Sunbelt Software

Antispyware

Protect Your Systems Against Spyware

Sunbelt Software's updated CounterSpy Enterprise 2.0 features a hybrid antispyware scanning and removal engine that combines traditional spyware protection and antivirus functionality. New scan and remove-on-boot technology detects and removes deeply embedded malware, and kernel-level active protection provides real-time signature-, behavioral-, and heuristic-based threat blocking and lets you prompt users to take action if suspicious behavior is detected. Other improvements include agent-scanning technology and automatic deployment functionality. A free trial version of CounterSpy Enterprise is available for download at http://www.sunbelt-software.com. For more information, contact Sunbelt Software at 727-562-0101 or 888-688-8457.

Authentication

Multifactor Authentication for Your Network

BioPassword announced BioPassword Enterprise Edition 3.0, a multifactor authentication solution for Active Directory (AD) and Citrix environments that uses biometric technology to authenticate users, not devices. The new version adds a layer of knowledge-based authentication to increase authentication accuracy and supports Windows XP Embedded thin clients and Outlook Web Access (OWA). BioPassword integrates with AD environments without requiring additional hardware or software. For more information, contact BioPassword at 425-649-1100 or go to http://www.biopassword.com.

Backup/Virtualization

Back Up Data from VMware VMs

The **STORServer** VCB Appliance uses VMware Consolidated Backup to centralize the backup of VMware ESX servers on the appliance, eliminating the need to have backup agents on each virtual or host machine. VMware Consolidated Backup creates a backup schedule for each virtual machine (VM). The appliance takes a snapshot of the VM according to the schedule, mounts the snapshot, then performs a full or incremental backup. Pricing starts at $20,000. Contact STORServer at 719-266-8777 or 888-786-7765 or visit http://www.storserver.com.

Exchange

Protect and Quickly Recover Exchange Server Data

Lucid8 released DigiVault 1.6, an Exchange Server continuous data protection (CDP) solution that features Single-Touch, a mechanism for rapid recovery of an Exchange database. DigiVault 1.6 speeds backups by a factor of 10 compared with earlier versions, and a new wizard-driven procedure makes setup easier. DigiVault 1.6 supports Exchange 2007, Recovery Storage Groups, and Windows Server 2003 x64. Pricing starts at $695 for 25 mailboxes. For more information, contact Lucid8 at 425-451-2595 or go to http://www.lucid8.com.

Special Operations Software™

Take Group Policy based systems management to the next level

White Paper: The Power of Group Policy

...Given the power of Group Policy, you'd think Microsoft would have done more to make it the very best management tool on the market for Windows systems. But, right now, there are still failings in the Microsoft GPO strategy. For example, if you want to **inventory your systems,** you have to use a different tool. That's a bit odd since AD already contains information about every single computer system in your network. Also, when deploying software through AD, there is no way to tell whether a software deployment actually occurred—except, of course, if you actually connect to the PC. That's because AD does not include any software deployment reporting features. And, if you **deploy 2007 Microsoft Office System** to your PCs, you'll find that you can't control how much bandwidth it takes or when the deployment begins. Your best bet is to start the deployment at night and hope it doesn't kill your network. It seems unfortunate that you would have to go through the entire process of designing and deploying your Active Directory and then find you need to perform another deployment just to implement a systems management tool. Fortunately, there is help...

About the Authors

Danielle Ruest and Nelson Ruest, MCSE, MCT, Microsoft MVP, are IT professionals specializing in systems administration, migration planning, software management and architecture design. They are also authors of multiple books.

DOWNLOAD the entire "The Power of Group Policy" White Paper at
www.specopssoft.com/winitpro

Microsoft GOLD CERTIFIED Partner

Security Solutions
ISV/Software Solutions

Call us at 866-857 5325 (Toll free)
www.specopssoft.com

EDITOR'S NOTE: Send new product announcements to products@windowsitpro.com.

Log Management

Search and Alert on Logs from Any Source

LogLogic's open log management and intelligence platform, LogLogic 4.0, now uses a service-oriented architecture and open API to let users create their own portals for compliance, risk mitigation, and forensics. The integrated Log Data Warehouse helps eliminate log silos by collecting and storing logs just once while allowing them to be shared many times. A Google-like multidimensional search on data helps accelerate IT forensics and improve compliance insight, and the Universal Log Processing feature extends reporting, search, and alerting capability to logs from any source—including homegrown and business applications—without requiring custom development. Contact LogLogic at 408-215-5900 or 888-347-3883 or go to http://www.loglogic.com.

Monitoring and Alerting

Monitor Server Environment Reliability and Performance

Neverfail Group announced an update to its Server Check Optimization Performance Evaluation (SCOPE) tool, which continuously collects and analyzes data about your infrastructure's hardware and software configurations, applications and system logs, and system performance. New features include continuous health checks and system monitoring of the server pair in a high-availability solution. SCOPE is available for 32-bit and 64-bit versions of Windows. For more information, contact Neverfail Group at 512-327-5777 or go to http://www.neverfailgroup.com.

Security

Ease Regulatory Compliance

Argent Software has announced updates to several products, including expanded Rule Sets for BlackBerry servers in Argent Guardian and support for all versions of Exchange Server in Argent Exchange Monitor. The company has also increased its network monitoring and compliance capabilities. Argent SNMP Monitor now includes customizable alerts to help you more quickly identify and react to network problems. Argent Data Consolidator, Argent Software's solution for complying with Sarbanes-Oxley Act and Health Insurance Portability and Accountability Act regulations, features Parse Sets to help you convey any type of logical expression. Each of Argent Software's solutions is managed using a centralized console. For more information, contact Argent Software at 212-710-0333 or 860-674-1700 or visit http://www.argentsoftware.com.

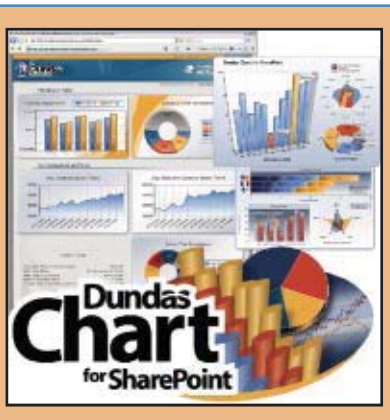
Security

Centrally Manage Peripheral Ports and Connected External Devices

GuardianEdge Technologies' GuardianEdge Device Control gives you a console for controlling user access to PC ports and the peripherals that are connected to them. With GuardianEdge Device Control, you can create access control policies to restrict the transfer of data between computers and removable storage devices or to block access to removable storage devices altogether. The product provides audit and alert capabilities for device usage across the organization and can produce reports that show audit permissions and the devices that are or were connected to PCs. Contact GuardianEdge at 415-683-2200 or 800-440-0419 or go to http://www.guardianedge.com.

SharePoint

Add Charts to SharePoint



Dundas Data Visualization announced Dundas Chart for SharePoint, a data visualization and charting component for Microsoft SharePoint technologies. Chart for SharePoint includes Asynchronous JavaScript and XML (Ajax) support, which lets you add interactive features such as tool tips, drill-down, zoom, and scrolling to charts. In addition to common pie, bar, and column charts, the product supports many advanced charts, such as box, polar, and radar charts. A standard license costs $1,999. For more information, contact Dundas Software at 800-463-1492 or go to http://www.dundas.com.

Storage

Reap the Benefits of DAS and iSCSI SAN

Zetera has released a line of NBOD ("networked bunch of disks") storage solutions for small-to-midsized businesses. Zetera NBOD combines the benefits of a SAN with the simplicity of DAS, enabling one or more servers to share storage on NBOD devices while requiring only basic networking skills for storage system deployment, configuration, and management. NBOD storage solutions are available in IU rack-mount ($2,699) and four-bay desktop ($2,199) models. For more information, visit Zetera's Web site at http://www.zetera.com.

InstantDoc ID 96190

Insights from the industry

Blending Identity and Network Management

AIO Networks (http://www.aIOnetworks.com), a networking and security solutions provider, listened to its customers when they asked, "How can you help us speed things up?" In the current IT climate, maintaining business continuity while upgrading to Web-based applications and implementing virtualization technologies is an important challenge. Merely buying more servers and bandwidth will only increase the complexity of network administration and management.

The EX Series appliance addresses WAN-based performance problems associated with bandwidth, visibility, and network control, and it does so by blending identity management with network management. EX Series appliances use link load balancing, compression, and cache redirection to provide advanced WAN optimization. The network intrusion prevention system (IPS) and firewall load balancing secure the network infrastructure, and SMP architecture provides scalability and reliability.

According to AIO Networks, EX Series is the world's only identity-based WAN utilization logging and reporting solution. It provides identity-based logging for file transfer applications such as FTP, Common Internet File System (CIFS), and NFS; email applications such as platforms SMTP and POP3; and IM platforms such as Yahoo!, AOL, and MSN. Identity-based bandwidth reports provide easy and instant visibility into what users are doing at a given time.

At press time, the EX Series was already available and EX Series 2.0 appliances were due for release at the end of May. Another exciting product that AIO Networks has released is the AX Series application acceleration switch. To read more about the AX Series and how it can improve user application response times by a factor of 8, go to http://www.windowsitpro.com and enter 95824 in the InstantDoc ID text box.

—Dianne Russell

InstantDoc ID 95824

DigitalPersona Takes Companies' Pulse on Authentication

Amr Assal, senior product marketing manager at **DigitalPersona** (http://www.digitalpersona.com), said his company wanted to find out what was on consumers' minds in terms of security and authentication. So, the company partnered up with Business Performance Management (BPM), surveyed both IT and security professionals, and discovered the following results. Of the professionals surveyed:

- 60 percent said that they or someone they knew in their company had shared a network password with a colleague.
- 83 percent said that compliance with government regulations is a top priority.
- Less than 50 percent had a security system or policy in place to create an electronic audit trail.
- 32 percent want security measures that combine ease of use and increased productivity.
- 29 percent see regulatory compliance as a top priority.

In the collected data, Assal sees an opportunity for DigitalPersona's enterprise, end-to-end, fingerprint solutions. Unlike passwords and smart cards, a fingerprint can't be shared with another individual. DigitalPersona can log all actions initiated with a fingerprint, such as accessing networked computers, and report on them to comply with federal regulations requiring an audit trail. Assal explained that DigitalPersona's solution can work with many of the built-in fingerprint readers that companies might already have in laptops, and with existing password-based authentication solutions.

—Renee Munshi

InstantDoc ID 95962

Quest Freeware Product Puts a Familiar, GUI Face on PowerShell

If the idea of using a command line to perform Exchange Server 2007 administration tasks scares you, a new freeware tool aims to allay that fear. **Quest Software** (http://www.quest.com) is offering PowerGUI, a free GUI front end for Windows PowerShell that lets you see as little—or as much—of PowerShell command syntax as you want. Dmitry Sotnikov, New Product Research Manager for Quest, explained that "the new interface provides an MMC-like console, to help [IT professionals] get familiar with [PowerShell] and learn the new syntax."

To put a more familiar spin on PowerGUI, Quest created an online community for users to discuss PowerShell, which also includes a link to download PowerGUI. Dmitry estimates that about one third of the PowerShell discussion activity is around Exchange 2007 administration and the other two thirds relate to using the command shell with Microsoft System Center Operations Manager 2007 and Active Directory (AD).

You might wonder (as I did) whether a graphical front end will remove administrators' incentive to learn to use PowerShell, but Dmitry believes that PowerGUI will instead help IT pros get used to working with PowerShell commands at their own pace, as well as use the GUI for certain tasks and the command line for others. "We don't see it as either/or. The command line and PowerGUI complement each other well," he said.

—Anne Grubb

InstantDoc ID 95821

JOIN US THIS FALL IN LAS VEGAS AT THE CUTTING-EDGE EVENT FOR IT PROFESSIONALS!

Over 240 in-depth sessions from Microsoft and industry experts, 150 speakers, and exciting announcements!

MICROSOFT EXCHANGE Connections 2007

WINDOWS Connections 2007

SharePoint Connections 2007

Office Connections 2007

November 5-8, 2007

LAS VEGAS, NEVADA

Mandalay Bay Resort and Casino

CONNECTIONS RAISES THE BAR FOR IT CONFERENCES, DELIVERING:

- EXPERT SPEAKERS
- UNPARALLELED WORKSHOPS
- DYNAMIC CONTENT
- HOT LOCATION

Co-located with

Microsoft ASP.NET Connections
Visual Studio & .NET Connections
SQL Server Connections
Mobile Connections

EARLY

EARLY BIRD BONUS

Register and book your room by July 15th and receive a **FREE NIGHT** at Mandalay Bay!
(based on a 3-night minimum stay)

REGISTER TODAY!

THIS EVENT SOLD OUT LAST FALL!

WinConnections.com ■ 800-505-1201 ■ 203-268-3204

Microsoft® Windows IT Pro TechNet MAGAZINE TECH Conferences Inc. PENTON MEDIA

Log Management Products for SMBs

These products make it easy to monitor and manage your event logs

by John Green

EDITOR'S NOTE: This is a summarized version of John Green's comparative review of log management tools for small-to-midsized businesses (SMBs). You can read the full version online by going to http://www.windowsitpro.com and entering InstantDoc ID 95955.

Event log management is important, but turning all the raw data from event logs into useful information isn't always easy. You can use event log information to determine why something didn't work as expected, to detect unauthorized activity, to monitor the health of systems and applications, and to archive and report information in support of regulatory compliance. The management of event logs is the common thread linking the six products that I've reviewed for this article. All the products support Windows event log and syslog monitoring and archiving, and several offer additional monitoring functions.

It's important to note that because Windows Vista's Windows Eventing 6.0 infrastructure significantly extends the capabilities of Event Tracing for Windows (ETW), specific Vista event log management support isn't yet available in these products.

Breakout Software MonitorIT 8.0.19

Breakout Software's MonitorIT 8.0.19 monitors not only Windows event logs but also syslog output; IP-based services such as SNMP, HTTP, FTP, SMTP, POP3, DNS, and Telnet; and SQL Server and Oracle database servers. This product also lets you create custom monitors for any IP port. Systems running the MonitorIT agent can also monitor services, processes, files, and performance counters.

MonitorIT is a server-based application that communicates with an agent installed on each monitored system. You perform most setup and administration tasks using a Web console. ActiveX Controls encrypt and transmit data between the console and the server via the agent port.

You can also use MonitorIT's Web console to create monitoring rules, called Watches. There are several types of Watches that you can configure. Server Watches monitor IP service ports such as email and Internet ports. SNMP Watches monitor SNMP traps sent to the MonitorIT server from authorized devices, and SNMP Counter Watches poll SNMP MIBs on remote devices. Syslog Watches receive syslog output from appliances and Linux/UNIX devices and have the ability to log all output to a text file and some events to the database. Each Watch type offers a variety of capabilities. For example, Process Watches will alert you to high levels of CPU and memory utilization, in addition to alerting you to the simple presence or absence of specific processes. Windows systems running the MonitorIT agent can load Event Log Watches, Process Watches, Windows Services Watches, File Watches, and Windows Performance Counter Watches onto the system. MonitorIT lets you configure Watches and alerts for custom Windows event logs in addition to the product's set of predefined standard event logs.

When you create a Watch, you can also configure its associated actions, called Alerts. Notification might occur via email, pager, syslog message, and SNMP trap. You can also execute a program or script on either the remote system by the MonitorIT agent or on the MonitorIT server.

MonitorIT uses a Microsoft Access format database by default but can use an ODBC database such as SQL Server. MonitorIT is licensed per monitored IP address. Breakout Software also licenses the application to Engagent, which markets the application as Sentry II.

MonitorIT isn't the ideal solution if event log reporting is your primary requirement because its strengths lie in system and application monitoring. This product had fewer predefined event log alerts and filters than the other products, and it doesn't let you create new Watches from existing event log entries. MonitorIT easily copies native Windows event log files to a central location for archiving but doesn't provide tools for archiving metrics written only to the database. This product is an effective, value-priced application, but expect to have to spend some time customizing your implementation.

Dorian Software Total Event Log Management Suite

Dorian Software's Total Event Log Management Suite comprises four separately available and installable components: Event Alarm, Event Archiver, Event Analyst, and Event Rover. Event Alarm 5.0 is a server monitoring and notification tool. Event Archiver 6.0 collects event logs for auditing and manages event retention in files and your database. Event Analyst 5.0 supports reporting against archived events in Total Event Log Management Suite–created databases and saved event log files.

SUMMARY

Breakout Software MonitorIT 8.0.19

PROS: Monitors a broad range of metrics in addition to Windows event logs and syslog output; the ActiveX-based Web console is responsive and easy to navigate

CONS: Relatively few predefined Watches and reports; no explicit procedures for archiving database-resident metrics

RATING: ◆◆◆◇◇

PRICE: Starts at $110 per server for 1–499 servers, $38 per server for 500–999 servers

RECOMMENDATION: Choose MonitorIT for an effective, value-priced alternative for system monitoring and log archiving, but expect to spend some time customizing your implementation.

CONTACT: Breakout Software • http://www.breakoutsoft.com • 908-561-5210

SUMMARY

Dorian Software Total Event Log Management Suite

PROS: Relatively easy to implement; flexible archiving options; custom reports; reporting procedures are the same whether selecting active logs, an EVT or CSV file, or a database source; agentless

CONS: If you purchase the full product suite, the modular design might add a few steps to your implementation

RATING: ◆◆◆◆◇

PRICE: Starts at $299 per server

RECOMMENDATION: Choose if you need only event log management without system monitoring features. The modular approach and support for SQL Server 2005 Express Edition will appeal to SMBs wanting to reduce their costs.

CONTACT: Dorian Software • http://www.doriansoft.com/totalsolution • 866-682-3646

Event Rover 1.1, which is intended for ad hoc analysis, retrieves and displays events remotely from active and saved event log files. Event Alarm, Event Archiver, and Event Analyst use a database—such as SQL Server, Oracle9i, or Access—to record and work with monitored event logs. Together, the four components monitor and manage Windows event logs and syslog output. Dorian Software licenses Total Event Log Management Suite on a per-monitored-server basis and lets administrators choose whether to install a software component locally or to monitor the server remotely. Syslog sources don't require a license.

Event Alarm, Event Archiver, and Event Analyst run as services. Event Alarm performs Windows event log monitoring without a client agent. Event Alarm receives syslog output and places the messages into the Windows application log, where the Event Alarm server processes them. Event Alarm includes many preconfigured alarms and lets you base custom alarms on recorded events. Named collections of alarms called Alarm Groups help you reduce your administrative efforts. Notification options might include one or more of the following notification methods: sending a message via email or to your pager, displaying a Windows console pop-up message on your desktop, sending messages to Event Alarm's Listener Console and syslog host consoles, and inserting the event into a database.

Event Archiver collects and consolidates Windows event logs by using the standard Windows event log API and shared folders, converting the EVT file to a comma-delimited format or loading the data into an Access, SQL Server, or Oracle database. Event Archiver will compress EVT files and move them to a network share or FTP server for long-term retention.

Event Analyst lets you view, report, and export event log information and connect to a Dorian Software Web site for more information about many event types. Event Analyst ships with many preconfigured basic filters to select events for display or reporting, many predefined report formats, and lets you create custom reports and write them to network shares in either HTML format or comma-delimited text file format.

Total Event Log Management Suite is an attractive event archiving and reporting solution. Its modular approach lets you purchase only the function you really need, which doesn't seriously complicate administration. Implementation is simplified by the lack of an agent. Overall, I found this product to be easy to use, with a useful set of predefined filters and reports and relatively easy procedures for creating custom filters and reports. This product is strictly a log management solution and lacks the system monitoring features I found in some of the other products.

GFI Software EventsManager 7.1

GFI Software's EventsManager 7.1 monitors and archives Windows event logs, syslog output, and World Wide Web Consortium (W3C) log file information. EventsManager is an agentless, server-based product and includes a large number of predefined filters, facilitating a quick implementation. Event filters let you configure real-time notifications for select high-priority events, and EventsManager suggests remedial actions for many events. A new add-on utility consolidates the event information that EventsManager servers collect at various company locations into a single database to help you manage database size and record retention. The separately installed GFI EventsManager ReportPack included in the license comes with a variety of predefined reports and enhances your ability to report on events that EventsManager collects.

To collect Windows EVT and W3C logs, the Event Retrieval Engine logs on to the remote system and uses standard Remote Procedure Calls (RPC) and the ETW API to retrieve event data by the schedule that you set. An Event Receiving Engine on the server acts as a syslog host to collect syslog information directed to it. EventsManager will process events against a set of rules and provides the option to archive the events to a SQL Server database. Another option lets EventsManager unconditionally archive all events for all specified logs on selected servers without invoking rules. When you call for the use of rules, EventsManager will filter out uninteresting events and alert you to selected events. Alerting actions include notification via email, Short Message Service (SMS), and Network Messaging (Net Send). You might also run a script or program to perform some remedial action.

Rules let you specify which event criteria will cause EventsManager to select an event for further processing. Rules can be organized into named rule sets for easy management and application. Monitored computers can also be organized within named groups. An event log

Learning Path

***WINDOWS IT PRO* RESOURCES:**

For more information about log management products:

"Security Log Collection," InstantDoc ID 93330

"Event Response," InstantDoc ID 44093

"Access Levels for Security Administrators," InstantDoc ID 93722

SUMMARY

EDITORS' CHOICE Windows IT Pro

GFI Software EventsManager 7.1

PROS: Many predefined events to facilitate implementation; a well designed, easy to navigate GUI console; many predefined display filters that can be easily augmented with custom display filters

CONS: The GUI console can't be installed remotely, so you must use a remote desktop product for remote administration; has a facility to log all events to the database but not to archive raw EVT files

RATING: ◆◆◆◆◆

PRICE: Starts at $800 for three nodes

RECOMMENDATION: Choose if you need to manage Windows event logs, W3C format log files, and syslog output.

CONTACT: GFI Software • http://www.gfi.com

scanning profile is a named set of rules and other configuration settings that you might apply to monitored computers or groups of computers. You can also apply several scanning profiles to a computer or a group, meaning you can augment profiles that apply to many or all systems with scanning profiles customized for a particular application or server. You can also browse and report on collected events stored in the database by using predefined or custom queries and event filters.

Overall, I was impressed by EventsManager and ReportPack. It's apparent that the designers had both ease of implementation and ease of use in mind when creating these products. The key area I felt EventsManager fell short in is its lack of support for remote workstation installation of the GUI console. I recommend EventsManager for anyone whose log management needs are limited to Windows event logs, syslog output, and W3C log file information.

Prism Microsystems EventTracker 5.6

Prism Microsystems' EventTracker 5.6 monitors and manages Windows event logs, several variants of syslog output, and text-based log files. The current version is about to be supplanted by EventTracker 6.0, which will offer full support for Vista's event channels. Prism Microsystems' EventLogCentral provides Web access for reporting and analysis to the data EventTracker collects. There are several optional components available that support server health monitoring and receive SNMP traps.

Prism Microsystems' EventTracker server is recommended for installation on Windows Server 2003 but is also supported by Windows XP and Windows 2000. It performs log monitoring with or without installing an agent on the monitored system. EventTracker consists of a Console Server, several services that run on the console server; three Web sites for remote administration and reporting; and agent services that run on monitored systems.

Data is stored in Microsoft-style CAB files, rather than in an ODBC-style database. Prism Microsystems determined that for log management, using a CAB data structure resulted in both disk space and performance advantages and eliminated the need for database management skills.

EventTracker lets you define access roles determining what users can do and permissions that specify what systems users can work with to support diverse needs within the organization, such as Help desk personnel and auditors.

The EventTracker Correlation Engine, EventTracker's rule-processing component, uses Linux/UNIX style regular expressions to match rules to events, a powerful, flexible approach to rule collection. When monitoring flat files, EventTracker maintains a bookmark to the file so it scans only new log information. Prism Microsystems includes knowledge modules to assist monitoring flat file logs that Microsoft IIS, SQL Server, and a few proprietary applications produce. EventTracker includes more than 500 predefined rules to facilitate rapid implementation.

As an event log monitor, EventTracker collects events from Vista, XP, Windows 2003, Win2K, Windows NT; syslog; Solaris BSM; SNMP; and any flat file log. In addition to log monitoring, agent-supported systems monitor CPU, memory, and disk utilization metrics; processes exceeding threshold; failing services; and network connections.

EventTracker has a lot of power and flexibility. At the same time, I found the UIs to be less intuitive to navigate than other systems. For example, if you want to add new monitored computers or groups, you must use the System Manager applet, rather than simply access the function from a right-click menu in the navigation pane. I created new system groups, yet they didn't show up in the auto refresh–designated navigation pane. In terms of response time, the console felt slow. I found myself waiting not only for event filters to take effect, but also when closing management applets. Overall, EventTracker boasts an impressive list of capabilities, but I found the organization and responsiveness of the UIs to be disappointing.

SUMMARY

Prism Microsystems EventTracker 5.6

PROS: Designed with a broad scope of capabilities; supports both agented and agentless monitoring; includes a Solaris agent; monitors some server health–related metrics; provides very flexible role-based access to the reporting and viewing console

CONS: Management UIs were a bit cumbersome, and the response time wasn't always good

RATING: ◆◆◆◆◇

PRICE: Starts at $9,000 for 20 Windows servers and 50 workstations. Contact vendor for more information.

RECOMMENDATION: This product's definable role-based authentication and Web console are attractive for Help desk use. If you need some of its unique features, I recommend that you install it for evaluation and see how it works for you.

CONTACT: Prism Microsystems • http://www.prismmicrosys.com • 443-539-3766

RippleTech LogCaster

RippleTech's LogCaster monitors and reports on activity in Windows event logs, device syslog output, and text file–based event logs. LogCaster stores logged events in a SQL Server database and uses SQL Server 2005 Reporting Services (SSRS) to create and save reports in several different formats, including PDF, HTML, or comma-separated value (CSV) file format. LogCaster's monitoring extends beyond event log data to monitor Windows performance counters running Windows services and network-based IP services such as email and Web servers on your network. In addition to Windows event log data and syslog output, LogCaster will monitor and report on IBM mainframe Resource Access Control Facility data.

LogCaster can be installed on XP, Windows 2003, or Win2K systems and requires SQL

SUMMARY

RippleTech LogCaster

PROS: Monitors services, performance counters, and IP-based ports in addition to events; supports remote console installation; supports distributed critical event management with the ability to send events to different consoles based on any event attribute; well-developed SSRS-based reporting suite

CONS: The ordered application of rules and lack of named rule sets can make administration and troubleshooting more complicated; LogCaster must write syslog output to a Windows event log if you want syslog events to be processed by rules and eligible for notification actions

RATING: ◆◆◆◆◇

PRICE: Starts at $550 for five licenses

RECOMMENDATION: Choose for a well-developed reporting suite, but be prepared for complicated implementation.

CONTACT: RippleTech • http://www.rippletech.com • sales@rippletech.com • 610-862-4000

Server 2005 or SQL Server 2000. SQL Server Desktop Engine (MSDE) is also supported.

The LogCaster service running on the LogCaster server communicates with agents to collect Windows event logs, manage the database, receive syslog data, and monitor performance counters and IP-based system health monitors. The LogCaster agent on monitored Windows systems receives event log filters (which have been configured for each system) from the server, processes and filters event log entries, and forwards select events to the LogCaster server. It also monitors any text files configured for Text File Watcher, a component that lets you search for specific text strings in the text file–based logs produced by many applications, including IIS. The agent also manages native event log file backups. The LogCaster server writes the event to a SQL Server database and performs any notification processing that you configured for the event. You can install the LogCaster Console GUI on workstations for remote administration.

LogCaster uses SSRS for reporting. RippleTech provides a large set of customizable reports. The Executive Dashboard is a particularly interesting report: It analyzes the information collected from all monitored systems and displays its assessment of system log policies that affect the integrity of Windows event log data.

For the most part, LogCaster is easy to use and includes a good feature set. The set of predefined reports is impressive, and because the reports are built around SSRS, they're relatively easy to modify. LogCaster supports many types of watches and monitors that go beyond mere event logs. Rules are relatively easy to configure, although it seems to me that the priority-based system might be somewhat hard to troubleshoot because there's no way to tell which rule processed an event. Performance-counter reporting isn't integrated with event reporting and is accomplished with a Microsoft Excel spreadsheet–based system. LogCaster has a nice set of features, but it seemed a little difficult to use at times due to the variety of configuration and display components in the console.

TNT Software ELM Log Manager 4.0

TNT Software's ELM Log Manager collects user-selected events from Windows event logs and file-based logs, receives syslog output from other systems and devices, and receives SNMP traps. Events are written to a SQL Server database for archiving and reporting.

The ELM Server supports agented and agentless monitoring. Windows systems have the ability to run a service agent, which provides the greatest functionality level. Virtual agents monitor Windows-based systems "agentlessly" through the use of remote procedure call (RPC) connections to the monitored system. IP virtual agents monitor non-Windows systems for syslog output and SNMP traps.

Monitor Items define what ELM Log Manager will look for in the stream of events generated on monitored systems. ELM Log Manager sends Monitor Items to systems running service agents; the agents evaluate events against the criteria set in Monitor Items and send selected events back to the ELM Server.

The ELM Server uses three SQL Server databases. The primary database is the repository for event information. The failover database, typically configured on the ELM Server, queues event information should the primary database become temporarily unavailable. To keep the primary database to a manageable size, ELM Log Manager lets you periodically move older events to an archive database.

Administrators use the Microsoft Management Console (MMC) ELM Log Manager Console GUI, which can be installed on other workstations for remote management. To configure log monitoring, you can create Agent Categories, assign monitored systems to one or more Agent Categories, and create and assign Monitor Items to those categories. The ability to assign a monitored system to several Agent Categories makes for flexible administration.

Although Monitor Items support a few kinds of notification, facilities of the Notification container of the console tree support fifteen distinct notification methods, including Marquee Display, text-to-speech (using the Microsoft Voice engine), and posting to a Web site. You can define Notification rules, which make use of event filters to describe which events each notification rule will apply to, and you can also define named notification methods to specify where notifications are sent.

I think most administrators will need to spend some time configuring ELM Log Manager to meet their needs because the default collectors are pretty generic. ELM Log Manager includes some nice features such as the automated collection configurations necessary for specific reports and the large variety of notification methods. I like ELM Log Manager's ability to configure multiple monitoring categories with assigned rule sets and to assign systems to multiple categories. The failover database is a great feature, if you care about the completeness of your log collection. I found the MMC to be well designed for easy navigation and administration. Overall, I found ELM Log Manager's capabilities—aside from the reporting—to be reasonably complete. Altogether, these features make ELM Log Manager one of the better products I reviewed for this article.

SUMMARY

TNT Software ELM Log Manager 4.0

PROS: Flexible event collection and alert definition; more supported notification methods than any other product; local failover database provides fault tolerance if SQL Server is temporarily unavailable

CONS: Few reports and no ability within ELM Log Manager to create new reports

RATING: ◆◆◆◆◇

PRICE: Starts at $325 for 1–399 servers, $215 for 400 plus servers

RECOMMENDATION: Choose ELM Log Manager for solid capability. Queuing events to the local failover database when the primary database is unavailable will help ensure the completeness of event collection, but you'll need to spend some time customizing the configuration and creating additional reports.

CONTACT: TNT Software • http://www.tntsoftware.com • 877-546-0878

The Bottom Line

As with any comparative review, I found that the six products here all have their benefits and drawbacks, and each product's feature set will draw different people to it. EventsManager 7.0 receives my Editor's Choice award because I was most impressed with its capabilities, including the flexibility with which you can use rules, rule sets, and scanning profiles; the variety of predefined rules and groups that facilitate startup; and the ease of routine reporting.

InstantDoc ID 95955

John Green
(john@nereus.cc) is the president of Nereus Computer Consulting.

Paul's Picks

Summaries of in-depth product reviews on Paul Thurrott's SuperSite for Windows

http://www.winsupersite.com

Windows Calendar

PROS: Free with Windows Vista, compatible with existing Web-based calendar standards

CONS: Consumer oriented, not centrally managed, no Microsoft Office Exchange compatibility

RECOMMENDATIONS: Although Microsoft Outlook likely meets the calendar needs of most IT pros, there's something to be said for free stuff. Vista users get a surprisingly full-featured calendar application, Windows Calendar, with their new OS. Unlike Exchange and Outlook, Windows Calendar fully adheres to the most popular Web calendaring standards, making it easy to publish and subscribe to calendars.

CONTACT: Microsoft • 800-426-9400 • http://www.microsoft.com

DISCUSSION: http://www.winsupersite.com/showcase/winvista_ff_calendar.asp

Windows Home Server Beta 2

PROS: Excellent workgroup backup capabilities, document and media sharing; comes in software-only version as well as bundled with server hardware

CONS: Beta 2 version isn't widely available; no Active Directory domain support; aimed at consumers

RECOMMENDATIONS: Windows Home Server takes the concept of Small Business Server (SBS) and scales it down, dropping domain support and enterprise server capabilities and adding the kind of functionality required by typical home networks. Home Server's excellent network-wide backup and imaging capabilities make it ideal for small workgroup setups. If you have simpler needs than even SBS meets, Windows Home Server might be an excellent solution.

CONTACT: Microsoft • 800-426-9400 • http://www.microsoft.com

SCREENSHOTS: http://www.winsupersite.com/showcase/whs_b2_gallery.asp

InstantDoc ID 95820

HP StorageWorks D2DI20

The **HP** StorageWorks D2DI20 is one of the latest products in HP's line of small-to-midsized business (SMB)–oriented storage devices. It's a disk-to-disk backup solution that provides backup capabilities for as many as four servers simultaneously. The unit I tested was a small floor-standing device about the size of a small tower PC. It provided 2TB of raw backup capacity that HP estimates is adequate storage for a month of data in a typical four-server environment. The unit came with four 500GB internal SATA disk drives. All of the disks in the D2DI20 were configured with RAID 5 to allow the unit to survive a disk failure and remain operational. The D2DI20's backup system emulates a Linear Tape-Open (LTO) tape autoloader drive by using the low-cost internal SATA drives for storage. This tape emulation lets the unit easily integrate into existing tape-based backup strategies—effectively replacing the tape drives—and still provide the advantages of disk-based backup. You access and manage the unit as if it's a tape device, so you can use it with existing hardware and backup software.

SUMMARY

HP StorageWorks D2DI20

PROS: Disk-based backup that's compatible with existing tape backup; easy management; can back up four servers simultaneously; holds a full month of backup data online

CONS: Setup requires Internet access to successfully complete; some incompatibility with Internet Explorer Enhanced Security Configuration

RATING: ◆◆◆◆◇

PRICE: $2,999

RECOMMENDATION: Investigate the D2DI20 if you're an SMB intending to upgrade from your existing tape-based backup solution.

CONTACT: HP • 800-752-0900 • http://www.hp.com

Setting up the D2DI20 was about as simple as it gets for a hardware unit. The system had two ports in the back. One connected to the power and the other connected the unit to the network. The network connection is a IGB iSCSI connector. I loaded the HP StorageWorks D2DI10/I20 Installation CD-ROM onto one of my network servers. The CD started an installation wizard that stepped through creating tape drivers for HP Ultrium tape devices on the server and locating the D2DI20 backup server on the network. I was prompted to supply a host name for the device and the IP address and my network domain name information. Finally, the wizard downloaded the Microsoft iSCSI Software Initiator, which is required to connect a client to an iSCSI target like the D2DI20 device. For some reason, instead of installing the iSCSI Software Initiator from the CD-ROM, the installation required an Internet connection to get the iSCSI driver, making an otherwise seamless installation dependent on external network configuration details. This portion of the installation failed for me, and I had to manually download and configure the iSCSI Software Initiator.

When the installation was complete, I used the Web-based D2DI20 Backup System Admin program to manage the device. The program added an icon to the desktop. However, launching the program from the desktop icon resulted in numerous Internet Explorer Enhanced Security Configuration errors. I could easily manage the device remotely, but to get the local Web management to work right, I needed to disable Internet Explorer Enhanced Security Configuration. Once I worked this out, I found the Web administration console to be very easy to use and understand.

The D2DI20 is compatible with existing tape backup tools. The unit came bundled with HP StorageWorks Data Protector Express backup software. Although the D2DI20 is intended primarily as a server backup unit, client systems can use their backup agents to connect to the device for backup. To test the backup capabilities, I loaded HP's StorageWorks backup program on the server. Data Protector Express is standard backup software that can be loaded on server or client systems; as client software, it runs on 64-bit hardware as a 32-bit application. It can use the D2DI20 as the backup target or it can back up to other targets, such as disks or other media. I found backing up to the D2DI20 to be extremely fast, as you would expect from a disk-based solution.

Apart from the minor installation problems I encountered, I found the D2DI20 to be fast, reliable, and trouble-free. The system is a huge step up from a traditional tape backup solution in speed and ease of use, yet is compatible with existing tape-based backup solutions. If you're looking for a reliable, hassle-free backup option that takes almost all the worry out of your SMB backup strategy, then I highly recommend checking out the D2DI20.

—Michael Otey

InstantDoc ID 96160

PrimalScript Universal

Whether you're a network administrator who's into scripting, or you're just getting into VBScript or PowerShell and you're looking for a more powerful and productive development environment, it's time to put away Notepad and take a close look at **Sapien Technologies**' PrimalScript. PrimalScript is the Rolls Royce of scripting editors. Like the Rolls, it's expensive, but it offers you features that you won't see from any of its competitors.

The PrimalScript Universal package contains way more than just an editor. It's a full-fledged development and training package, providing you with tools for writing administrative scripts as well as Web and .NET applications. The PrimalScript Universal package includes the editor PrimalScript 4.1 Enterprise, which is the primary script editor, as well as PrimalScope, a VBScript and JScript debugger. In addition, the package also includes multiple VBScript training CDs, including VBScript 101, 201, and 301, and PrimalScript 4: Untamed, a course for PrimalScript itself. Other reference sources include *VBScript Enterprise Best Practices, VBScript Advanced HTML applications (HTA) for Windows Administrators, Managing IIS with VBScript,* a one-year subscription to ScriptingAnswers.com, and a supplemental CD-ROM containing more than 200 additional code snippets.

Using an InstallShield setup program, the PrimalScript editor installed effortlessly in under a minute. You definitely get the feeling that PrimalScript is different from other editors beginning from the moment that you first start using it. Unlike most editors that start with a blank editing window, PrimalScript greets you with PrimalScript's User Interface Customization Wizard. This wizard lets you select the role you want to use. You have several options, including VBScript/Network Administrator, Classic ASP, and Minimum Default UI. Because I wanted to test the new PowerShell editing features, I selected PowerShell/Network Administrator. Next, you choose the layout you want, which essentially controls visibility of UI elements such as browsers and toolbars. Finally, you choose the file types that PrimalScript's Open dialog box will show. The wizard also can add an *Edit with PrimalScript* option to Windows Explorer's context menu. Using the wizard to customize the PrimalScript interface isn't a one-time deal. You can go back later and use the Tools menu to customize all of the settings available.

PrimalScript supports virtually all of today's popular scripting and programming languages, including VBScript, PowerShell WSH, JScript, JavaScript, Perl, PHP, KiXtart, and several other languages such as ASP, C/C++, C#, and VB.NET. In total, PrimalScript Universal provides language support and color-coded keywords for 46 development languages. PrimalScript provides all of the editing features you would expect, including support for unlimited undo and redo (including undo/redo support for past editing sessions), find and replace, support for recording and running macros, and syntax checking. PrimalScript also provides many advanced editing features such as code completion, code folding, source control integration, visual file comparison, a COM library browser, a code snippet library, and Windows Management Instrumentation (WMI) and Active Directory Service Interfaces (ADSI) wizards. It also provides several additional useful features, including optional line numbering, bookmarks, and a hexadecimal display mode.

The total number of features is too lengthy to discuss them all here. The features in the PrimalScript package are unrivaled in any of today's scripting editors.

For the Windows administrator, PrimalScript is particularly well suited for VBScript development. The VBScript snippets and multiple wizards make VBScript development very productive, plus the included VBScope debugger is powerful and easy to use. PrimalScript's support for PowerShell is good but it isn't as mature as the VBScript support. It has code coloring, syntax checking, and code completion but no debugging. You can use PowerShell's built-in Set-PSDebug, but that rudimentary tracing option isn't really comparable to PrimalScope's VBScript debugging capabilities.

PrimalScript 4.1 is a powerful and feature-rich editor. However, I found the $1,369 price for PrimalScript Universal to be too steep. The PrimalScript Universal package is best suited for the beginning Windows administrative scripter who needs training resources and wants to focus on VBScript. For experienced scriptwriters I recommend the less expensive Professional edition, at $279. Although $279 for PrimalScript Professional might seem like a lot compared with free editors, PrimalScript 4.1 delivers the tools to make it worthwhile for the serious scripter. To download a 45-day trial version for the Standard, Professional, or Enterprise editions, go to Sapien's trial download Web site (http://www.primalscript.com/downloadtrial.asp).

—Michael Otey

InstantDoc ID 96035

SUMMARY

PrimalScript Universal

PROS: Full-featured editing environment, PowerShell support, VBScript debugging, extensive VBScript training and reference materials

CONS: Expensive, no PowerShell debugging, no PowerShell training or reference materials

RATING: ◆◆◆◆◇

PRICE: $1,369

RECOMMENDATION: PrimalScript Universal is best suited to IT professionals who want VBScript training in addition to a full-featured development environment. Experienced scriptwriters would find Sapien's other package, PrimalScript Professional, to be a better value.

CONTACT: Sapien Technologies • http://www.sapien.com

KVM over IP Switches

Get out-of-band access to system KVM functions at any location, any time

In our February 2006 issue, we gave you a "KVM over IP Switches" buyer's guide (InstantDoc ID 48825) that showcased the products of nine major vendors in the field. Now, nearly a year and a half later, we'd like to revisit the market—share some new offerings from favorite vendors as well as introduce you to some newcomers. KVM over IP technology is one of the most fundamental components in your network infrastructure, so we like to keep our finger on the pulse of the industry and get you the information you need to make the right buying decisions.

The Benefits

It's easy to see how KVM over IP functionality can improve IT efficiency: KVM over IP switches give you out-of-band access to system keyboard, video, mouse (KVM) functions, from any location at any time. You're probably constantly challenged to get past geographic barriers in your day-to-day network management, needing to find quicker ways to react to problems on far-reaching systems. Or perhaps you're one of only a few IT administrators at a small-to-midsized business (SMB) or branch office, and you need to increase productivity despite your lack of resources. A KVM over IP switch lets you easily maintain and manage geographically diverse devices, better manage systems to reliably deliver key business services, and drastically reduce total cost of ownership (TCO).

KVM over IP switches give you access to and BIOS-level control of connected servers and other network devices straight from your desk or any other location: You can securely manage your entire IT infrastructure—including branches and remote data centers—through the use of one central interface, as if you were administering them locally. You can even provide external modem support if the network fails and you can no longer use remote-access software.

Making the Choice

How do you choose the right KVM over IP switch for your environment? The switches from various vendors can differ substantially. If you choose the wrong switch, you'll waste valuable resources and possibly even compromise your business's security. To choose correctly, you need to keep in mind some key factors.

The solution you choose needs to be able to support every OS platform and network device contained in your environment. As Web Table 1 (http://www.windowsitpro.com, InstantDoc ID 96095) shows, most of these vendors' solutions support a broad range of platforms, including Linux, Sun, and Macintosh. You might not have some of these platforms in your local environment, but don't forget that your network probably knows no boundaries: You must also consider remote users' laptops and mobile devices.

You need to decide how many ports you want the switch to have. Will you need it to handle more as your company grows? Is the switch scalable? How does the switch handle video? What's the maximum video resolution? Check to see what type of video compression the switch offers for conserving bandwidth. Another feature you might find useful is sound capability. You also need to consider the form factor of the hardware (is it rack mountable?), the type of cables you'll need for server connections, the maximum number of simultaneous sessions, and the maximum distance the switch allows between the switch and servers. And what kind of failover functionality does the switch provide? Effortless, reliable access to critical resources is a key feature of a KVM over IP platform.

Some switches offer client-side software for communicating with the KVM switch, whereas others make do with an Internet browser to perform the same function. You need to weigh the pros and cons of both approaches. If you prefer limited user access to the switch, client software is better for your environment. But if you need to give administrators access regardless of location, a browser-based interface is the best bet.

Finally, keep in mind the importance of security. A major byproduct of the KVM over IP switch's inherent centralization is tighter control of your widespread resources, but the various solutions available today take differing approaches to security. Determine whether the switch takes advantage of your existing authentication technologies or uses its own methods. Does the switch encrypt all signals between itself and managed devices? A great deterrent to intrusion is an encrypted administrative GUI.

Start Here

Your KVM over IP switch is one of the most important pieces of your IT architecture, giving you anytime, anywhere, out-of-band, BIOS-level access to your widespread network's most basic functions. Of all your IT resources, KVM technology is one area where you don't want to choose unwisely.

InstantDoc ID 96095

Jason Bovberg (jbovberg@windowsitpro.com) is a senior editor for *Windows IT Pro* and *SQL Server Magazine*. He has more than 10 years of experience as a writer and editor in magazine, book, and special-interest publishing.

EDITOR'S NOTE

The Buyer's Guide presents vendor-submitted information. To find out about future Buyer's Guide topics or to learn how to include your product in an upcoming Buyer's Guide, go to http://www.windowsitpro.com/buyersguide.

THE 4 Pillars OF SYSTEM CENTER CONFIGURATION MANAGER

BY ED ROTH

Microsoft has christened System Center Configuration Manager (SCCM) 2007 as the new incarnation of its vaunted System Management Server (SMS). The System Center moniker acts as an umbrella that covers Microsoft's family of manageability tools. Along with Configuration Manager, the current list of System Center solutions includes Operations Manager, Data Protection Manager, Reporting Manager, Essentials, Virtual Machine Manager, and Capacity Planner. The company also recently announced a new Help desk offering called System Center Service Desk (SCSD). But SCCM is the senior member of the System Center lineup, and it's arguably the anchor component.

Let's take a look at SCCM's architecture and the solid set of tools it provides for managing your entire Windows infrastructure, highlighting some of the new and exciting features of SCCM 2007. Then, let's drill down into what you need to know about putting the new generation of Microsoft systems management software to work in your environment.

Built on 4 Pillars

SCCM is a major retooling of previous SMS technologies and capabilities. In its introduction of the new product, the Microsoft product team uses an analogy of four pillars upon which the new system is built. The pillars are *simplicity, deployment, security,* and *configuration.*

Simplicity. The simplicity pillar represents a worthwhile goal for a product with so many capabilities. Toward this end, Microsoft has rolled feature packs and add-ons into the core product so that administrators no longer need to find, download, and integrate such tools individually. A new setup routine tracks and displays setup tasks as they occur and builds a management point so that the SCCM installation is

The new SMS incarnation promises simplicity, comprehensiveness, security, and manageability

ready to begin client deployment following setup. Microsoft has also introduced the notion of maintenance windows and integrated Wake on LAN (WOL) capabilities, both of which let SCCM administrators more easily control when and how the tool's operations occur on managed systems. The Microsoft Management Console (MMC) 3.0–based UI, which Figure 1 shows, gets some terrific enhancements, including drag-and-drop and search folders. Microsoft has streamlined many administrative tasks with dynamic wizards to reduce the complexity of operations. Another great new feature—Volume Shadow Copy Service (VSS)–enabled backups for SCCM site systems—further simplifies administrators' lives.

Deployment. The deployment pillar focuses on making SCCM a complete solution for deploying both server and desktop OSs throughout the enterprise, in addition to applications and updates. These capabilities have existed in some fashion in SMS 2003, but Microsoft has redesigned them to integrate the latest Windows OS deployment technologies—such as Windows Preinstallation Environment (PE), Windows Imaging Format (WIM), and User State Migration Tool (USMT)—into an unattended OS deployment process. The product uses a task-sequencing engine during the deployment process to ensure that necessary steps (e.g., installing drivers and applications, restoring user documents and settings) occur.

Security. The security pillar is primarily composed of two security initiatives that make SCCM a better tool for managing security updates for your enterprise and make the SCCM infrastructure more secure than previous SMS versions. The first initiative involves enhanced vulnerability assessment and remediation technology, and the second initiative involves seamless, end-to-end, mutual authentication between SCCM systems and managed clients—whether they're connected via the Internet or on the LAN or roaming between the two.

Configuration. The configuration pillar entails giving IT organizations the ability to model and manage a desired configuration for a given system type.

Figure 1: The SCCM 2007 UI

IT Pro Hero

Scripting Eases an SMS Migration

BY B. K. WINSTEAD

Server specialist Stefan Suesser developed a toolkit to automate his firm's transition from SMS 2.0 to SMS 2003

Stefan Suesser faced a potentially daunting challenge: As the server expert on his IT department's infrastructure design team, he had to craft a way to migrate his company from Microsoft Systems Management Server (SMS) 2.0 to SMS 2003, since no third-party SMS 2.0–SMS 2003 migration tools exist. Stefan works for Computacenter, a well-known European provider of IT infrastructure services. Its central IT department, located in Kerpen, Germany, supports around 220 servers in the data center (most running Windows Server 2003), in addition to servers at the branch offices. With so many servers, SMS migration wouldn't be a trivial affair. Fortunately, Stefan was well qualified to script a migration solution, having achieved 100 percent in the advanced categories of VBScript and Windows PowerShell at Microsoft's 2007 Scripting Games. In a recent conversation, Stefan explained to me the components of his solution and how it works.

Q: Why did you decide to upgrade to SMS 2003?

A: Computacenter Germany introduced SMS 2.0 in 2001. Over the years, we realized that our SMS 2.0 implementation wasn't optimal, so we came up with a plan to start from scratch, implement a new and simplified SMS 2003 infrastructure, and leverage new features such as Advanced Client, software update management, Active

SCCM administrators can create management policies to establish a baseline for system-configuration items, including hardware configuration, installed software, system load, and specific settings. The system can report on compliance with the baseline configuration and can take knowledge-driven actions based on particular out-of-compliance conditions.

Core SCCM Features

Total cost of ownership (TCO) was once a huge driver for promoting tools to better manage IT systems, but the term TCO seems to have fallen out of vogue. However, we should never underestimate the necessity of keeping the cost of managing desktop and server systems in check. IT organizations are responsible for maintaining a healthy TCO bottom line.

That's where SCCM comes in. SCCM is geared toward increasing the overall effectiveness of IT organizations, streamlining provisioning, and managing computing resources while minimizing the overhead of doing so. The following core SCCM features all contribute in the effort of accomplishing these lofty goals: software distribution, inventory and reporting, device management, OS deployment, software update management, remote tools, desired configuration management, network access protection, and Internet-based client management.

Background Intelligent Transfer Service (BITS) and maintenance windows ensure that software installation doesn't hamper a user's productivity.

Software distribution and updates. Software distribution is a huge part of SCCM and has been since the first version of SMS. Software distribution is the ability to remotely deploy software—typically an application—to one or more client systems. That summation sounds simple enough, but modern businesses' software-deployment needs reach far beyond simply installing a given software package onto a group of desktop computers. Attention must be paid to a target system's connection type, system type, and usage pattern, as well as the overall bandwidth of the network you're using for delivery. Furthermore, once you've installed a software package, it will likely need updates over the course of its service life. You can use collection machine variables—which help you categorize computers based on certain parameters (e.g., OS, memory, disk)—to ensure that SCCM targets only appropriate systems for certain software. Background Intelligent Transfer Service (BITS) and maintenance windows ensure that software installation doesn't hamper a user's productivity. If an uncooperative user insists on powering off his or her system each night, you can use WOL to power it on for software maintenance. SCCM uses binary deltas—with DFS replication (DFSR) hashing—to minimize the bandwidth impact of application updates for sites and distribution points across your network. (A binary delta copies only changed bits of an application update. For example, if you have a 700MB Microsoft Office package and you need to change one file, only the differences in that file will need to be transferred for the entire package to be current—as opposed to the entire 700MB package.)

Inventory and reporting. Even small IT shops can have trouble getting a clear picture of the hardware and software assets that comprise their fleet. SCCM's inventory and reporting features help with this challenge. You can configure the inventory component to collect hardware and software information from client systems at a prescribed interval. The reporting component then assembles appropriate pieces

IT Pro Hero

Directory (AD) integration, and protected distribution points. Software updates and patches were a major concern because Computacenter used a homegrown patch-installation mechanism that didn't scale to our needs; if we had stayed with SMS 2.0, a major redesign of the tool would have been necessary.

Q: How long did it take to develop the migration tool? How does it work?

A: The development of the migration toolkit, which consists of a number of files and scripts, took me about six weeks, including testing. I decided to use an XML file to store information about the SMS objects, obtained via Windows Management Instrumentation (WMI). To use the WMI namespace on the SMS site server, you have to connect to the \\root\sms\site_xxx namespace, where xxx is the site code of your SMS implementation. You can then use all the available classes to read or manipulate SMS objects (we used VBScript files to do so). We used VBScript scripts to connect to WMI on the SMS 2.0 source server and read all the relevant information into the XML file—collections, packages, programs, and advertisements together with attributes such as ID, descriptions, and so on. This is where an XML file is handy because you can store the objects with their relationships better than you could with an Excel spreadsheet or something similar.

The script that re-creates the collections on the new SMS 2003 server reads the information from the XML file to do its magic. It writes back the resource ID of the newly created collections into the XML file. After all collections are created, the script restores the original hierarchy of collections.

We used another script to export all packages and advertisements into Managed Object Format (MOF) files. MOF files are text files, so you can manipulate them and recompile them on the new SMS 2003 server to create these objects.

We then used a script that leverages mofcomp.exe, the MOF compiler, on the new SMS 2003 site to add the packages into SMS. This script writes back the new package ID into the XML file. We had to update the advertisement MOF files with the new collection ID and package ID, information already stored in the XML file. After the script updated the

Learning Path

WINDOWS IT PRO RESOURCES:

"System Center Essentials Beta 2007," InstantDoc ID 94762

"Microsoft Updates Management Roadmap," InstantDoc ID 95590

"MOM Management Packs," InstantDoc ID 94671

"MOM for SMBs," InstantDoc ID 94361

"QUARANTINE!" InstantDoc ID 50386

MICROSOFT RESOURCES:

"System Center Configuration Manager 2007 Beta" http://www.microsoft.com/technet/sms/2007/evaluate/download.mspx

"Configuration Manager Documentation Library" http://www.microsoft.com/technet/prodtechnol/sms/smsv4/smsv4_help/6ffe5c59-3858-49c5-83cb-16f63823187c.mspx

of the collected data into meaningful reports. These reports can be quite simple (e.g., a breakdown of desktop computer platforms) or quite complex (e.g., HP laptops in the accounting department with a specific BIOS version and video driver version, running Microsoft Internet Explorer—IE—7.0 on Windows XP SP2). Software-inventory and software-metering reports can also help you get a firm grasp on license management.

Device management. Device management—which Microsoft really should call *mobile* device management—originated as a feature pack add-on to SMS 2003. The company has enhanced the feature and incorporated it into SCCM. Device management lets you perform on mobile devices management functions similar to those available to traditional clients. For example, you can perform hardware and software inventory, file collection, software distribution, settings control, and password management. Current SCCM-manageable devices include those running Windows Mobile software on Pocket PC, or smart phones and devices running Windows CE. The SCCM documentation—accessible from the Learning Path—contains an exhaustive list.

OS deployment. SCCM's OS-deployment capabilities add up to a dramatically enhanced version of the SMS 2003 feature pack add-on and solution accelerator. These new core functions are based on OS deployment technologies in Windows Server 2008 and Windows Vista. Using the OS deployment tools, you can build a reference machine and capture a single image of it for deployment to an entire enterprise. SCCM supports such deployment scenarios as bare-metal installations, in-place upgrades, and machine-to-machine migrations.

Software update management. SCCM leverages Windows Server Update Services (WSUS) as the underlying technology for updates and patches. However, you'll use the SCCM interface to wield enhanced control over the approval and application of updates. Additionally, SCCM's update-management features give you a means with which to deploy updates from third-party and internal software providers and—for the purpose of compliance—allow for tracking and reporting of updates applied throughout your enterprise.

Remote tools. The ability to remotely control managed systems has been a long-standing, useful SMS feature for troubleshooting and providing end-user support. Microsoft has revamped SCCM's remote tools so that, by using Vista's RDP protocol, they realize the benefits of improved performance, security, and richer collaboration technologies. SCCM also still supports Remote Desktop and Remote Assistance.

Desired configuration management. Every IT organization recognizes the benefits of standardizing systems and configurations. SCCM's desired configuration management component—previously an SMS 2003 solution accelerator, now enhanced and integrated into SCCM—lets you define a model for the configuration of a certain class of system. SCCM will then monitor managed systems for compliance according to that definition.

Network access protection. Microsoft's Network Access Protection (NAP) is an entirely new feature in SCCM. In simple terms, NAP is a tool for monitoring your network for noncompliant, potentially vulnerable systems, and proactively correcting any potential compliance problems before

IT Pro Hero

MOF files, it again invoked mofcomp.exe to add the advertisements to SMS and wrote back the new advertisement ID into the XML file. And, as one of the last steps, we had to change the download behavior of the advertisements so that clients remote to the distribution point would download and run the program.

These steps describe the migration tool set in general—there were other necessary steps that dive deeper into the SMS nuts and bolts. The entire migration requires you to perform one step after the other in the right order—for example, you have to create the packages first, then change the advertisement MOF files with the new package ID before you can create the advertisements.

Q: How long did the migration take?

A: The migration took only about an hour in production! Without the migration tool set, our administrators would have had to create all the SMS objects manually—with more than 1,000 objects, this would have been a long and error-prone process.

Q: Are you planning to migrate to the next version of SMS, System Center Configuration Manager 2007?

A: Yes, we're currently evaluating Configuration Manager 2007. When performing an upgrade, we want to do an in-place upgrade and hopefully won't need to use the migration tool set. However, although I haven't tested it, I assume my tool set can be used with Configuration Manager 2007 because the WMI classes are still the same.

InstantDoc ID 96143

B. K. Winstead
(bwinstead@windowsitpro.com) is an assistant editor for *Windows IT Pro* and *SQL Server Magazine.*

Read the expanded version of this article at http://www.windowsitpro.com, InstantDoc ID 96143.

_INFRASTRUCTURE LOG

_DAY 74: This is too much. We're stuck dealing with multiple interfaces and apps. We can't find the relevant info we need. I feel like it takes six of us to do one person's job.

_Six Gils? They better not all have to sign my time sheet.

_DAY 76: I'm taking back control with IBM WebSphere® Portal. It's the fastest and easiest way to integrate everything so we have seamless access to our information. Like Web 2.0 for the business environment, it gives each and every one of us a single, customizable interface.

_Back to one Gil. There's so much less of him to love now.

WebSphere® Portal

IBM.COM/**TAKEBACKCONTROL**/INTEGRATION

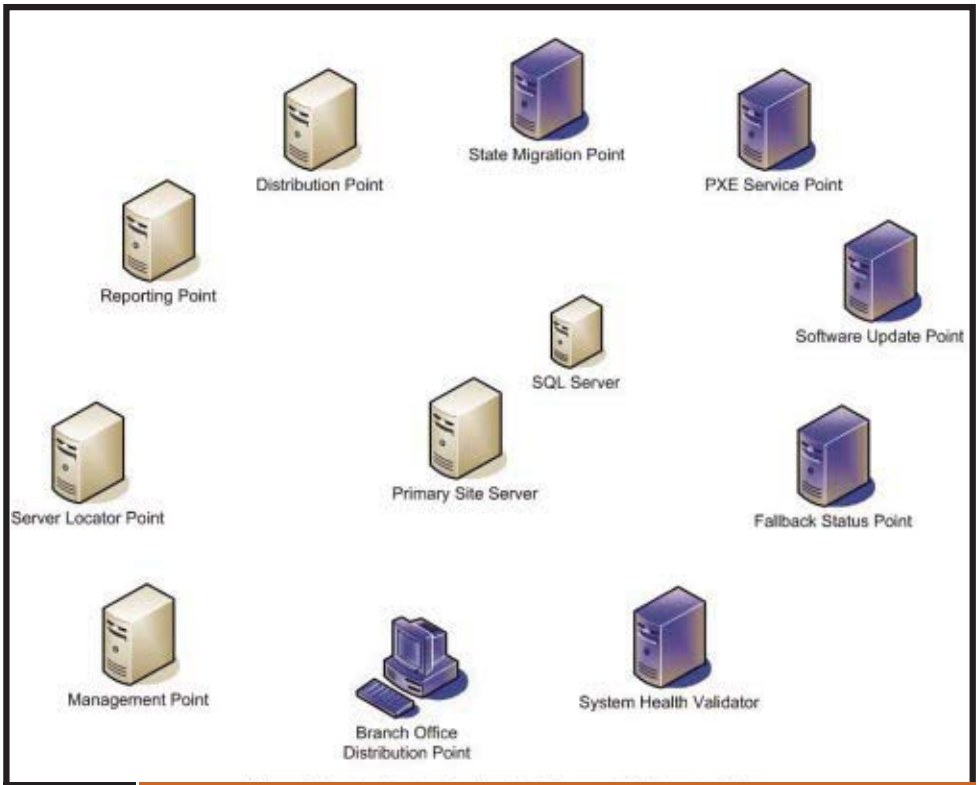


Figure 2: The SCCM 2007 system roles

permitting such systems network access. However, NAP implementation requires Windows Server 2008 to be running Network Policy Server. NPS policies measure system compliance, and SCCM's NAP performs any required remediation.

Internet-based client management. Although SMS has traditionally managed many types of clients—including desktops, laptops, and servers—the ability to manage portions of the client population connected via the Internet has been lacking. SCCM has incorporated secure Internet-based management capabilities into the core feature set. Using public key infrastructure (PKI), clients can securely participate in traditional software deployments, inventory schedules, and other SCCM functions while connected only via the Internet.

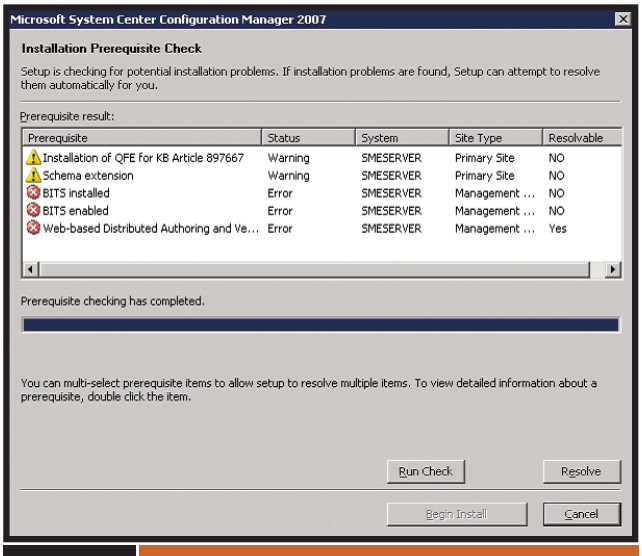


Figure 3: SCCM's Setup Wizard checking for prerequisites

What You Need to Know

Now, you're probably wondering what else you need to know before taking the SCCM plunge—either as a new deployment or as an upgrade to an existing SMS installation. For new deployments, the first thing you need to consider is the size and complexity of your environment, and whether you require and can benefit from SCCM's extensive management capabilities. If you read my beta review of System Center Essentials (see the Learning Path), you might remember that tool's limit of 30 servers and 500 client systems. Those numbers also serve as a reasonable point at which implementing SCCM starts to make sense: If you have fewer than 500 systems, you might not benefit from the robust, complex beast that is SCCM. If you have an existing SMS implementation, an upgrade to SCCM should be on your radar at release time. After you make the decision to move to SCCM, you'll want to spend some time on two preparatory steps, involving PKI and site system roles.

PKI. Of primary concern, if you don't have an existing PKI implementation, you'll need to learn about the technology and deploy PKI to support SCCM's advanced security features. PKI is a requirement for native-mode deployments (i.e., full deployments of SCCM clients and required servers) because the system uses a site server signing certificate to sign all SCCM policies. Through this infrastructure, site systems and managed clients establish mutual trust.

Site system roles. Your next area of study is site system roles. SCCM offers numerous new roles and dispenses with or renames a few old ones. Although adding new roles might seem to contradict the goals of the simplicity pillar, Microsoft has designed the roles to help you better manage and maintain your SCCM infrastructure and managed systems.

As you see in Figure 2, the SCCM 2007 system roles are primary site server, site database server, Configuration Manager console, *branch office distribution point, fallback status point, management point, PXE service point, reporting point, server locator point, software update point, state migration point,* and *system health validator.* Note that not all roles are necessary, and each role doesn't need to reside on a dedicated server. In fact, for very small implementations, it's feasible—but not recommended—that all required roles reside on one server. Your determination of appro-

priate roles and supporting hardware will be a factor of your environment's workload and security requirements. You can find many planning aids for SCCM deployment in Microsoft's Configuration Manager Documentation Library (see the Learning Path), which can help you come up with the right mix of roles and hardware.

Two new roles of note are branch office distribution point and fallback status point. A branch office distribution point (which replaces the old *secondary site* role) can be a Vista or XP system. This system can hold software applications and updates for distribution to a branch office. SCCM utilizes BITS technology to initially populate and apply delta changes to software on branch office distribution points. SCCM uses the fallback status point as a catchall for communications from managed systems that have somehow become orphaned from their intended management point. This system role is instrumental in discovering and fixing client-reporting problems in your fleet.

Installation Considerations

You'll want to become familiar with the various installation options available to you, depending on your current situation. If you're installing a brand-new SCCM 2007 site, you have two options—simple setup and custom setup—although the simple setup isn't very useful unless you're deploying for test purposes. SCCM's Setup Wizard checks for prerequisites (as Figure 3 shows), helps you mitigate any software deficiencies, then walks you through the process of specifying site and managed system parameters. If you already know exactly how you want to deploy SCCM, you can streamline this process by using the scripted installation option.

If you're upgrading an existing SMS 2003 site, you have a number of options, decisions, and prerequisites to consider. First, before you can add SCCM to the mix, your SMS 2003 site must be running SMS 2003 SP2. Second, SCCM doesn't support Windows 2000 servers, so you'll need to upgrade any SMS systems running on that OS. Third, you need to decide whether you'll use a side-by-side or in-place upgrade strategy.

Organizations that aren't heavily invested in their current version of SMS will find the side-by-side upgrade acceptable. This upgrade amounts to bringing up the new SCCM site, then reassigning and upgrading existing managed systems to the new site. More probable though, is an in-place upgrade. An in-place upgrade migrates your existing data to the new database schema and lets you run in an interoperable mode while you convert to SCCM 2007. One caveat is that the upgrade process removes any unsupported feature packs—particularly those for OS deployment and device management. However, although the upgrade removes the legacy feature packs, their functionality is replaced natively in SCCM 2007, and the new SCCM-native features will use the settings previously configured for the feature packs.

When you upgrade, you should go from the top of your hierarchy down. One helpful tip is to consider placing a central SCCM 2007

site above your existing SMS 2003 primary site, then let your data flow up. Using this scenario, you can familiarize yourself with the new SCCM console while using your own data. From the SCCM 2007 console, you can view—but not edit—SMS 2003 site settings. You can upgrade secondary SMS 2003 sites to SCCM 2007 manually, by pushing them via SMS, or by installing them through remote control. You can assign SMS 2003 clients to SCCM 2007 sites, and SCCM 2007 clients—in mixed mode—can roam back to an SMS 2003 site for interoperability.

Client-Deployment Considerations

You can assign SCCM clients based on AD OUs so that the assignment strategy can be more aligned with the structure of your business than an SMS site structure. In addition to standard push-client installations and software distribution methods, there's a new way to perform client installation. Using the Software Update Point, you can piggyback on your WSUS implementation to overcome client-installation obstacles such as account permissions and unopened ports. When Microsoft releases SCCM to manufacturing, the company will provide an .adm template for distributing SCCM client settings via Group Policy.

Microsoft has also made notable improvements to the SCCM client-installation executable. The tool uses a single binary file—ccmsetup.exe—for all client installations. The new executable has bandwidth awareness through BITS, and it downloads a simple XML manifest first to determine which components are applicable to a given client, then downloads and installs only what is necessary.

Other Caveats

SCCM's native mode and the PKI infrastructure it requires are requirements for Internet-based client management. Also, you're going to have to modify your AD schema to use NAP, but that prospect isn't as scary as it might sound. If you're comfortable with it, you can run the ExtADSch.exe file (from \SMSSETUP\BIN\I386) on the SCCM 2007 installation media, or you can use a Microsoft-provided LDF file. The LDF file documents the classes and attributes added in the process of modifying the schema, as well as the SCCM features they're associated with. (NAP is one such feature that requires an update to the AD schema.)

Worthwhile Investment

Microsoft's investment in its four-pillar strategy of simplicity, deployment, security, and configuration should pay dividends for IT organizations ranging in size from medium to huge. Existing SMS users will benefit greatly from an upgrade to Microsoft's latest and greatest configuration management tool, and SCCM's new capabilities and usability add up to a compelling argument for deployment in many IT organizations where previous versions of SMS might not have made the cut.

InstantDoc ID 95959

Ed Roth

(eroth@windowsitpro.com) is a network manager for a government institution and a contributing editor and product reviewer for *Windows IT Pro*.

POCKET THE PROS

Ordering the SQL Master CD is like pocketing a team of SQL experts.

Packed with thousands of articles, bonus content, and loads of expert advice—getting the SQL Master CD is like pocketing your very own team of professional SQL consultants.

And at a fraction of the cost.

Search for articles by keyword, subject, author or issue. Get real-world solutions in lightning-fast time—order the SQL Master CD today.

Only $59.95

POCKET ONE TODAY!

www.sqlmag.com/go/pocketpros 1-800-793-5697

SQL Server magazine

LET WDS EASE YOUR VISTA ROLLOUT PAIN

BY JOHN SAVILL

SOLUTIONS SNAPSHOT

PROBLEM:
Deploying Windows Vista to enterprise computers

SOLUTION:
Use Windows Deployment Services to implement an image-based OS installation.

WHAT YOU NEED:
Windows Server 2003, Windows Automated Installation Kit, Vista installation media, a reference computer, a central deployment computer

DIFFICULTY:
●●●○○

Although the Windows OS has evolved significantly over its lifetime, the Windows installation process has remained virtually unchanged. Media containing compressed versions of the files comprising the OS are installed and uncompressed one by one, then the install process detects hardware and performs configuration. Likewise, the method of network installation, Remote Installation Services (RIS), has changed little since Microsoft introduced it in Windows 2000. The Windows installation process is slow, both over a network and via physical media because it requires the installation and configuration of numerous small, isolated components one at a time. This design has the advantage of isolating each component so it can be easily changed without affecting the rest of Windows, but it also produces a lengthy installation process.

All this has changed in Windows Vista. In developing the Vista installation process, Microsoft went back to the drawing board. All Vista installations use an imaging process, which essentially allows a reference machine to be installed and configured, then executes a program (usually Sysprep) to wipe machine-uniqueness information and prepare the OS on the machine for duplication, and finally captures the reference system's contents to a file, which contains the OS to deploy on clients.

To better support this image deployment environment, Microsoft created Windows Deployment Services (WDS), which is a new deployment tool that replaces RIS and is compatible with Vista's new Windows Imaging Format (WIM). Although these technologies have made installing Windows much easier, there's still a lot to learn, so let me walk you through the process of preparing your custom OS installation image and deploying it to client machines over the network.

Install WDS

WDS runs on Windows Server 2003, and will be a core part of Windows Server 2008 (formerly code-named Longhorn). It's available as part of the Windows Automated Installation Kit (WAIK), which you can download from http://www.microsoft.com/downloads/details.aspx?FamilyID=c7d4bc6d-15f3-4284-9123-679830d629f2&DisplayLang=en, and although it's a very large download (more than 800MB), it includes everything you need to deploy Vista, including:

- The WDS update for Windows 2003 SP1 servers with RIS. You must install RIS prior to installing the WDS update on Windows 2003 servers in both 32-bit and AMD 64-bit versions
- Whitepapers and documents about using WAIK and WDS
- Vista-based Windows PE (WinPE) environments, which help you create bootable media to capture and deploy images
- The Windows System Image Manager, which you use to create the automated answer XML files that you can use with WDS and to add or modify components (e.g., drivers) in the images
- Various tools including the ImageX command-line tool, which you use to capture and deploy WIM

OS deployments have a new image

images, as well as mount WIM images to the file system to enable easy manipulation of the WIM content

After you download and install the WAIK, you need to install WDS on the Windows 2003 server from which you'll deploy the OS image (if you're running Windows 2003 SP1—Windows 2003 SP2 comes with WDS). To install WDS, navigate to the WDS folder of the WAIK media and run the .exe file for the processor type (i.e., 32-bit or 64-bit) update. Accept the license agreement and reboot your server.

WDS on Windows 2003 runs in one of three modes—Legacy, Mixed, or Native—to enable backward compatibility with existing RIS-based installations that you might still need to deploy and support. To learn more about these modes, see the Web-exclusive sidebar "WDS Server Modes," http://www.windowsitpro.com, InstantDoc ID 96099. You can check which mode a server is running in by right-clicking the server in the Microsoft Management Console (MMC) Windows Deployment Services snap-in (which you'll find in the Administrative Tools menu after you install WDS) and selecting Properties. The mode is shown on the General tab, as Figure 1 shows. You can also check the mode by using the following command:

```
wdsutil /get-server /show:config
```

Configure WDS

To run in any mode other than Legacy, you'll next need to configure WDS. (Note that WDS on Windows 2008 will support only Native mode and deploy only WIM OS installations.) You can configure WDS by using either the command line or the Windows Deployment Services snap-in. For this article, I outline the snap-in method, so launch the snap-in from the Administrative Tools menu and perform these steps:

1. Right-click the WDS server and select Configure Server, which opens the Windows Deployment Services Configuration Wizard. Click Next.

2. The wizard displays the network requirements (i.e., the computer must be member of an Active Directory—AD—domain, you must have a DHCP server and a DNS server on the network, and you need an NTFS partition for image storage). Click Next to indicate you have these prerequisites.

3. Enter the path to a folder where you'll store the images that WDS will use, which best practice dictates shouldn't be the system drive (and your system will warn you if you enter such a path). Click Next.

4. On the DHCP Option 60 screen, you'll see options to make WDS listen on port 60 rather than the regular port 67 and to configure DHCP to tell Preboot Execution Environment (PXE) clients to communicate on port 60. If DHCP is installed on the WDS server, you need to select the *Do not listen on port 67* option. If you're using Microsoft DHCP, also select the *Configure DHCP option 60 to PXEClient;* otherwise, you'll need to manually configure the option on your DHCP server.

5. Next, select options for how the WDS server responds to clients (i.e., respond to no clients, known

Figure 1: Showing the server is running in Native mode

SOLUTIONS SNAPSHOT

SOLUTION STEPS:

1. Download and install WAIK.
2. Install and configure WDS.
3. Prepare the boot environment.
4. Create an OS installation image.
5. If necessary, create a capture disk for nonnetworked computers.
6. If desired, create and install an answer file for unattended installs.
7. Deploy the Vista image to client computers.

clients, or all clients), depending on the security of your environment. There's also a suboption that requires WDS to wait for administrator approval before responding to unknown computers. Click Finish.

6. You now have the option to add images. I prefer to clear the *Add images to the Windows Deployment Server now* check box and manually add the images later. Click finish.

Add the Boot Environment

You now have a WDS environment, but you're missing two critical components: a bootable environment to which to send the PXE clients to allow the deployment of images and the Windows images themselves. WinPE is the environment WDS uses to deploy images, and although the WAIK installs a WinPE version that's based on Vista into the Tools\PETools\<processor architecture> subfolder of the WAIK installation, this version isn't suitable for use with WDS. The Vista-based WinPE included with WAIK is perfect for building media that you can use with the rest of the WAIK (e.g., the ImageX command that you use to capture and deploy images), but it doesn't contain the WDS client binaries that are needed for WDS to function. Instead, you need a WinPE version that's based on Windows 2008. The boot.wim file in the Sources folder of the Vista media is a WinPE version that's based on Window 2008 and includes the WDS client binaries.

You can add a new WinPE boot image to WDS by right-clicking the Boot Images leaf in the left panel of the WDS snap-in and selecting Add Boot Image. After you specify the name and location of the boot image to add (e.g., D:\sources\boot.wim), click Next and enter a name and description. The default is the name contained in the WIM file, for example, "Microsoft Windows Longhorn Setup (x86)." However, you can change the name to anything you want (e.g., "Microsoft Windows Deployment Services environment"). Then select the WIM images to install (although the WinPE WIM image file consists of only one image), and click Next to copy the WIM file to the Boot\<architecture>\Images subfolder of the RemoteInstall folder selected during WDS configuration.

Add the Installation Image

You now have a boot image that clients can use to boot via PXE into the WDS deployment environment. The next step is to add an OS installation image, which in this case is Vista. To add the image, open the Windows Deployment Services snap-in, right-click the Install Images leaf of the navigation panel, and select Add Install Image. You'll be prompted to select an Image Group to add the image to or to create a new Image Group (e.g., Windows Vista). Click Next and select the name of the WIM file to import (e.g., the install.wim file in the Sources folder of the Vista DVD). Remember, WIM files are an XML type format that can contain more than one image. The Vista WIM file contains all the available versions of Vista (except Enterprise). However, because the different versions share much of the same content, the WIM format can take advantage of Single Instance Storage (SIS) technology and the total file size is smaller than you'd expect. Clear the check boxes of the versions you don't want to make available. When finished, click Next to display a summary of the selected versions. Accept by clicking Next, and the Add Image Wizard will perform an integrity check on the selected WIM file and import the images.

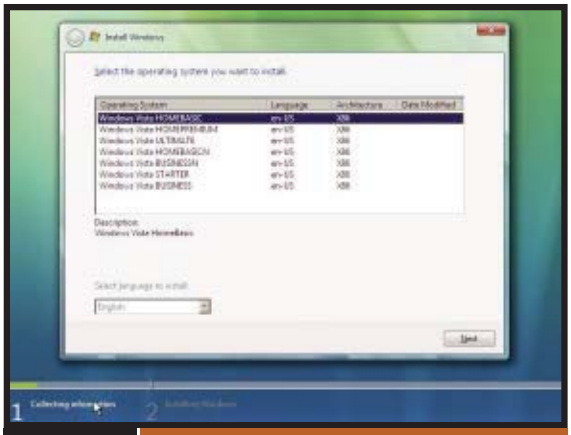


Figure 2: Selecting an OS to install

Now when you boot a PXE-enabled client, you're prompted to press F12 to boot to WDS (which will be familiar to users of RIS). Select the basic language settings and the credentials to use in the domain. Then select an OS from the list of OSs known to WDS, as Figure 2 shows, and click Next. You'll be prompted for a partition to install to, then WDS will install the OS, asking minimal information such as registered owner and time zone information.

The WAIK includes the Windows System Image Manager, which lets you create the XML answer file that automates OS installation.

There's also a version of the boot ROM that doesn't require you to press F12. To use that version, right-click the WDS server in the Windows Deployment Services snap-in and select Properties. Select the Boot tab. Click the Browse button next to the appropriate client architecture, and select the .n12 version of the boot ROM (e.g., instead of pxeboot.com, use pxeboot.n12). Now, you'll no longer need to press F12 to boot to WDS.

Discover Images and Unattended Installs

You now have a WDS installation that can deploy Vista over the network, but what about machines that can't boot over the network? WDS has a bootable media (called Discover boot image) for machines that don't natively support booting over the network. The Discover boot image CD-ROM lets you avoid having to load WinPE over the network. To create a Discover boot image CD-ROM, right-click the Windows 2008-based WinPE under the Boot Images section of the Windows Deployment Services snap-in and select Create Discover Boot Image. Enter a location and filename for the new WIM file, along with the WDS server to contact for OS images, as Figure 3 shows.

Next you convert the WIM to an ISO file so that you can burn it to a CD-ROM to enable bootable deployment. To convert the WIM file, follow the steps outlined in the article "Windows Deployment Services Update Step-by-Step Guide for Windows Server 2003" at http://technet2.microsoft.com/Windows-

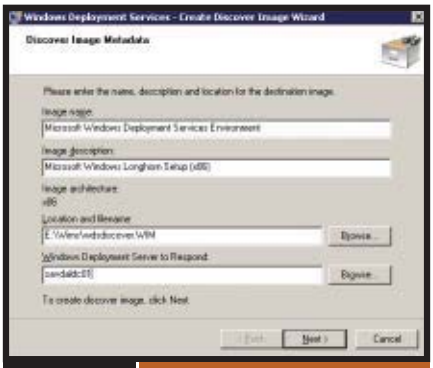


Figure 3: Creating a discover image

Vista/en/library/9e197135-6711-4c20-bfad-fc80fc2151301033.mspx?mfr=true.

Finally, how do you avoid having to enter information during the installation? The WAIK includes the Windows System Image Manager, which lets you create the XML answer file that stores custom settings and automates OS installations. The use of the Windows System Image Manager is beyond the scope of this article, but you can find instructions and a list of settings and values in the "Unattended Windows Setup Reference" Help file that ships as part of WAIK.

In the initial WDS stage in which you select the OS that you want to deploy, you assign the answer file you created by selecting the Properties of the WDS server. Under the Client tab, select the *Enable unattended installation* and select the answer XML file for the architecture. To select the answer file for a particular image, right-click the image and select Properties from the Install Images, Image Group section. Then under the General tab, select the *Allow image to install in unattended mode* and select the XML install file to use (which must be part of the RemoteInstall folder structure where images are stored). You can now deploy Vista without having to enter information with each installation.

Getting Better All the Time

WDS is a powerful component of Windows 2008 and Windows 2003, giving us a unified method to deploy both server and client OSs. If you've been using RIS, then WDS will be far more intuitive. The next step is to look at the Business Desktop Deployment (BDD) 2007 solution accelerator which builds on technologies such as WDS and Microsoft Systems Management Server (SMS) to help in the complete desktop deployment experience, including inventory of existing systems, application packaging, hardening the desktops, and following a best practice deployment. The BDD will be the focus of a future article.

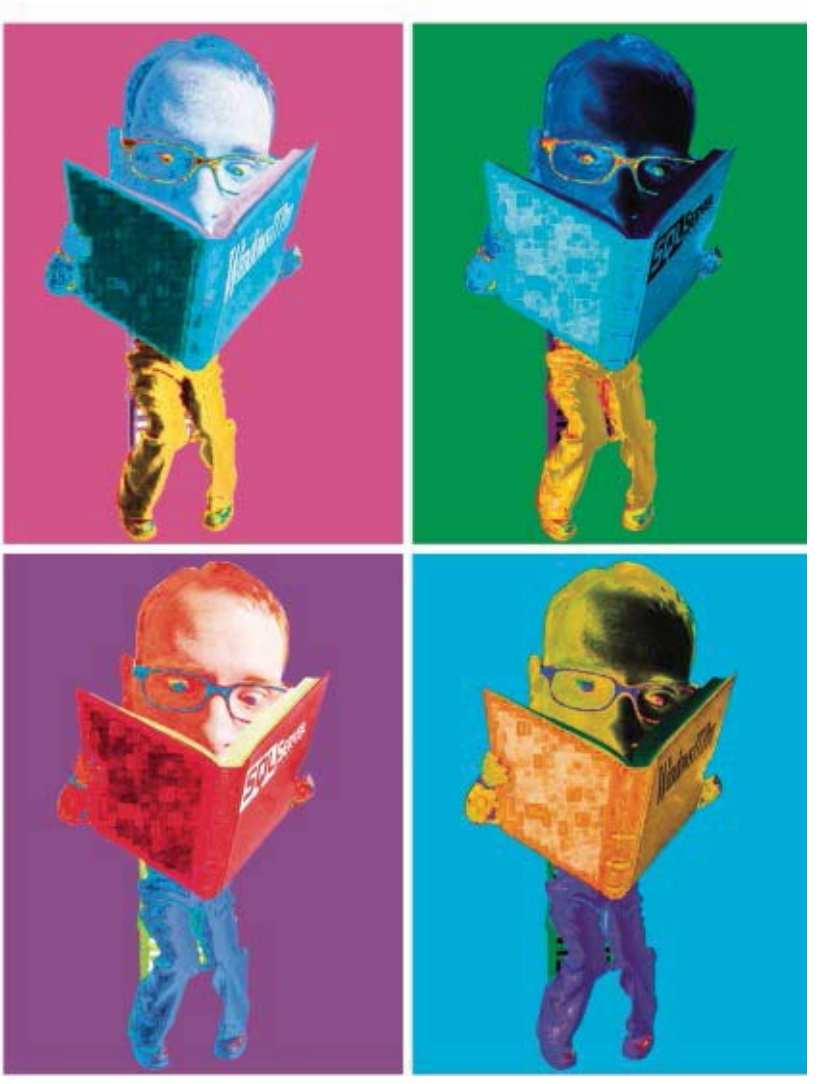
InstantDoc ID 96098

John Savill

(jsavill@windowsitpro.com) is Director of Technical Infrastructure for Geniant. He is a CISSP, a Security and Messaging MCSE on Windows Server 2003, an eight-time MVP, and a Krav Maga instructor. He is also the author of *Windows Server 2003 Active Directory Design and Implementation from Packt Publishing* (http://www.packtpub.com/book/active_directory) and is currently working on a comprehensive Windows Server 2008 publication.

"In the future, everyone will be world-famous for 15 minutes."

-Andy Warhol, innovator



So when is it your turn?

Have you or your staff come up with an innovative IT solution? If so, you could win a *SQL Server Magazine* or *Windows IT Pro* 2007 Innovators Award for it! In addition to bragging rights and fame, prizes include complimentary airfare and conference passes to Fall Connections in Las Vegas, write-ups in upcoming magazine issues, and more!

Windows IT Pro INNOVATORS AWARDS 2007

SQL Server INNOVATORS AWARDS 2007

To enter and view complete rules, visit
www.windowsitpro.com/awards/innovators_2007.cfm
or www.sqlmag.com/go/innovator

Innovators Contest entries will be accepted May 1 through August 1, 2007. Winners will be notified by August 17, 2007.

Safely Deploy Security Templates

The *Windows Server 2003 Security Guide* gives you some powerful tools—use them wisely

BY RUSSELL SMITH

In addition to providing valuable guidance for hardening your Windows Server 2003 systems, Microsoft's *Windows Server 2003 Security Guide* contains a series of security templates that you can apply to servers in your environment according to their role. You can choose from three categories of templates:

- Legacy Client (LC) for environments still running legacy applications that aren't compatible with standard security settings
- Enterprise Client (EC) for environments aiming to implement the standard level of security recommended by Microsoft
- Specialized Security – Limited Functionality (SSLF) for high-security environments in which limited functionality is acceptable

For each template category, the guide provides templates for such roles as Domain Controller, Member Server, File Server, and Web Server. Using the templates, you can quickly comply with Microsoft's best practices on a single server or across a series of servers through Active Directory (AD) and Group Policy (GP).

But isn't Windows Server 2003 secure out of the box? And if so, why would you need to use these security templates?

Windows Server 2003 is indeed more secure than any previous version of Windows Server, but different server roles have varying security requirements. And there's still a huge range of additional security settings that you can configure for your particular needs.

In addition, by using these templates to configure server security, you can control, manage, and enforce your servers' security configuration from a central location—AD. Instead of having different or unknown settings that are manually configured (or not controlled by policy) on every server, you can be sure of the configuration and easily manage it.

Although the templates give you an easy way to comply with Microsoft's best practices and simplify configuration management, deploying the templates can create compatibility problems with other applications and affect functionality. To successfully deploy the templates, you need to plan for them early in the security design stage as well as understand the changes they make to your systems and how to roll them out without affecting functionality. You also need to know how to override the templates to meet your organization's security needs.

Inside the Templates

When you deploy the *Security Guide* templates, they configure four main areas of security. Those areas are

- Account Policies (Password, Lockout, Kerberos)
- Local Policies (Audit, User Rights Assignment, Security Options)
- Event Log
- Restricted Groups

Unlike previous versions of the *Security Guide,* Version 2.1 doesn't include a System Services section for defining services and related security settings. Now, you need to either define the settings for each service manually or use the Security Configuration Wizard (SCW) to create a Group Policy Object (GPO) that is based on combined settings from a security template and the wizard's recommended configuration for services when you run it against a reference machine. You can also use the SCW to add Windows Firewall and IPSec configuration settings to a GPO.

The settings configured under the Account Policies, Event Log, and Restricted Groups sections are relatively straightforward and shouldn't cause many problems as long as you understand how the features work. (You can read an overview of the *Security Guide* at http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx.) However, User Rights Assignment and Security Options settings under the

WINDOWS SERVER 2005 SECURITY GUIDE

Read the overview at http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx

Download the Security Guide and its tools at http://www.microsoft.com/downloads/details.aspx?FamilyId=8A2643CI-0685-4D89-B655-52IEA6C7B4DB

Do's and Don'ts of Using Security Templates

DO

Incorporate security templates in your Group Policy design from the very beginning.

Test all policies in a preproduction lab environment.

Use the SCW to configure start-up settings for system services.

Create a backup (including a system state backup) before deploying GPOs created from the templates in a production environment.

Consider using the templates in conjunction with Group Policy to secure and manage your environment.

Read the documentation that comes with the *Windows Server 2003 Security Guide*.

DON'T

Deploy a new GPO created from a security template and/or the SCW in your production environment without extensive testing and approval from system stakeholders.

Dismiss the risk to functionality of deploying security settings from a template en masse in a production environment.

Make changes to your production environment without a proven roll-back plan.

Table 1: NTLM Settings Before and After Deployment of the EC – Member Server Template

Group Policy Setting	Configuration Before EC – Member Server Template Is Deployed	Configuration After EC – Member Server Template Is Deployed
Network security: LAN Manager authentication level	Send NTLM v2 responses only	Send NTLM v2 response only, refuse LAN Manager
Minimum session security for NTLM Security Support Provider (SSP)–based clients (including secure remote procedure call—RPC)	No minimum	Require message integrity Require message confidentiality Require NTLM v2 session security Require 128-bit encryption
Minimum session security for NTLM SSP-based servers (including secure RPC)	No minimum	Require message integrity Require message confidentiality Require NTLM v2 session security Require 128-bit encryption

Local Policies section can cause functionality problems in your environment if you don't plan for them carefully.

For example, deploying the EC – Member Server security template to a member server running Exchange Server 2003 could limit or break your Exchange Server functionality. If Exchange SMTP is configured to accept connections using Windows Integrated Authentication from a server in another Exchange organization, the EC – Member Server security template will prevent SMTP communication between the two servers. The SMTP queue will begin to fill up, and your email won't go anywhere.

Windows Integrated Authentication for Exchange SMTP relies on legacy NTLM authentication, and at the root of the problem are the NTLM settings configured in the EC – Member Server template. Table 1 describes the NTLM configuration before and after the template is deployed. As you can see, in an environment where the EC security templates have not been deployed, there are no special requirements for NTLM session security. However, the EC security templates configure the maximum security requirements, causing Windows Integrated Authentication on Exchange SMTP connectors to fail.

However, as we'll see in a moment, you can override the templates' security policies for particular servers to maintain needed functionality.

Deploying the Templates

As you can see from the Exchange SMTP example, a couple of simple tweaks to server security can spell disaster for server and application functionality. Ideally, you should plan for and integrate the templates into your Group Policy design at an early stage, testing all functionality before going live. After you've moved an environment into production, implementing the changes required to deploy these templates becomes very difficult.

Whether you deploy the templates in the early stages of a system's life or after the system has gone live, you must thoroughly test the GPOs in a lab environment to ensure that functionality isn't affected.

Because the templates use many additional registry values that are not true Group Policy

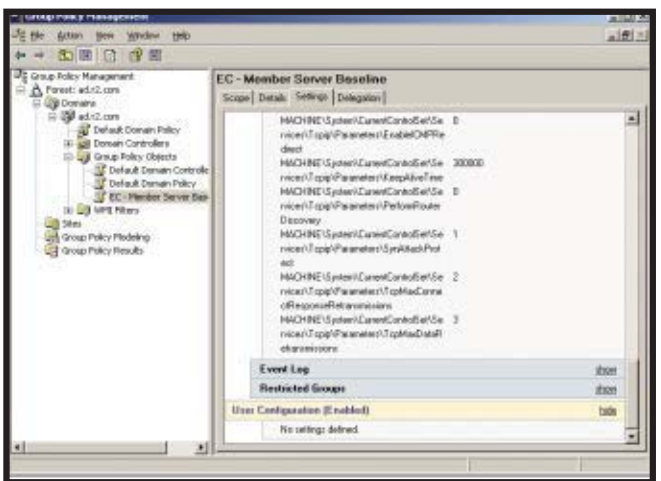


Figure 1: Additional registry settings for TCP/IP security

settings—and thus can't be reversed by simply unlinking the policy—you must back up your system (including the system state) before deploying policies created by using the templates. The \Software\Policies and \Software\Microsoft\Windows\CurrentVersion\Policies subkeys under HKEY_CURRENT_USER and HKEY_LOCAL_MACHINE are the only places where true, non-persistent policies are defined. Figure 1 shows some examples of TCP/IP parameters that are configured in other areas of the registry. Because the TCP/IP parameters defined in the template are not located in the areas of the registry mentioned above, the changes will be persistent and can't be reversed by removing the GPO.

Creating a New GPO

You should always create new GPOs for deploying the *Security Guide* templates. Don't import settings into existing policies such as the Default Domain Policy. Importing settings into an already configured policy (unless you clear the security database beforehand) will create a confusing combination of settings from the template and the original policy. For ease of use and management, the policies should be unique known quantities, as defined in Microsoft's documentation. You should also retain the original configuration of the Default Domain Policy in case you need to roll back to the previous configuration.

Before you start to configure the new policy, you need to choose (or create) a reference machine that has the same general configuration as the machines to which you want to deploy the policy. For instance, if you want to deploy a policy to Exchange servers in your organization, the reference machine should have Exchange installed and all necessary services running.

Let's walk through using the SCW to import template settings into a new GPO along with recommended System Services start-up settings by using a reference machine. Before working through the following steps, install the SCW from Add/Remove Windows Components under the Add/Remove Programs Control Panel applet. You also need to download the *Security Guide* (available at http://www.microsoft.com/downloads/details.aspx?FamilyId=8A2643C1-0685-4D89-B655-521EA6C7B4DB) and install the guide and its tools.

1. Start the SCW from Control Panel, Administration Tools. Click Next on the Welcome screen.

2. Select *Create a new security policy,* and click Next.

3. Select the name of the reference machine. Use Browse if the machine you're running SCW on is not the reference machine. I recommend that you run SCW from the reference machine instead of remotely because certain files are required on the local machine if you are configuring IIS security, for example.

4. When security database processing is complete, click Next until you reach the Selected Server Roles screen.

5. Ensure that the selected server roles are the ones you want the server to perform, and click Next.

6. Confirm the installed features and options, and click Next.

7. Review additional services, and click Next.

8. Decide whether to leave the additional services as is or disable them, and click Next.

9. Review the changes that will be made to the start-up type of each service listed, and click Next.

10. Skip the configuration of Network Security, Registry Settings, and Audit Policy, and click Next until you reach the Security Policy File Name screen. (Configuring network security is outside the scope of this article, but of course, you should configure it as part of this procedure. Registry Settings and Audit Policy are already configured in the security template, and SCW should not override those settings.)

11. Click the Include Security Templates button, and then click Add.

12. Browse to the location where you installed the *Security Guide* templates and select the *.inf file for the role and security level you want to configure—for example, EC-Member Server Baseline.inf. Click OK.

13. In the *Security Policy file name* text box, save the new policy file to the root of your C drive (e.g., c:\ec_memberserver) and click Next.

14. Select *Apply later,* click Next, and then click Finish.

To convert the resulting SCW *.xml file into a GPO, open a command prompt and execute the following command:

```
scwcmd transform
  /p:c:\ec_memberserver.xml
  /g:"EC – Member Server Baseline"
```

When the command has completed, you will see the new EC – Member Server Baseline policy in the Group Policy Management

Table 2: Three Settings for the SMTP Override Policy

Group Policy Setting	Exchange SMTP Override Settings
Network security: LAN Manager authentication level	Send NTLM v2 responses only
Minimum session security for NTLM SSP-based clients (including secure RPC)	No minimum
Minimum session security for NTLM SSP-based servers (including secure RPC)	No minimum

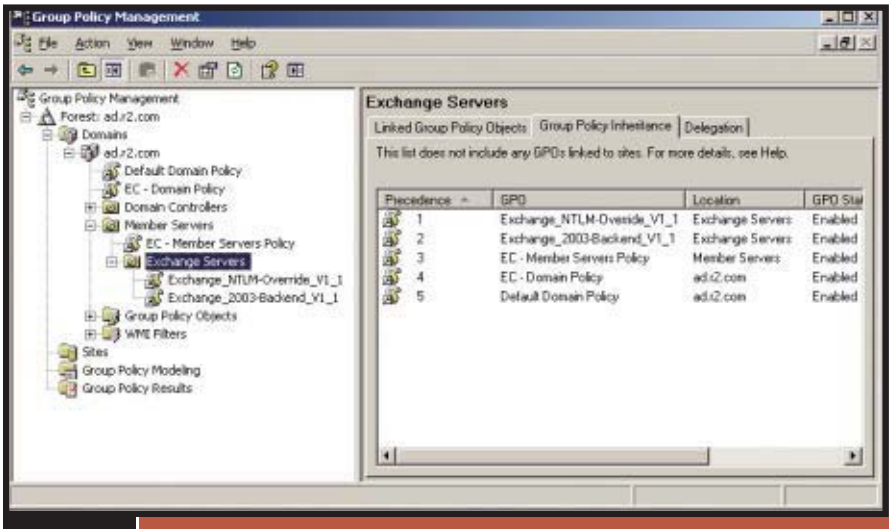


Figure 2: Linking security policies by precedence

Console (GPMC) under the Group Policy Objects node for the domain. (Note that there is a bug in GPMC when used on Windows Server 2003 Release 2. If you use GPMC to view the settings for the new policy, System Services are not displayed. However, if you view the policy using Group Policy Editor, you will see that System Services start-up settings have been defined in the policy.)

Creating Override Policies

To resolve the problem with SMTP functionality that we looked at earlier, you can create a new GPO called an *override policy* that you apply only to the affected servers. The override policy contains just a few modifications to lower specific security requirements for the affected servers and leave the other configuration settings intact. The policy is then applied with a higher priority than the EC – Member Server policy to ensure that the modifications are implemented successfully. In the SMTP example, the override policy contains only the three settings that Table 2, page 47, shows.

Figure 2. page 47, shows how you can use the Group Policy Management screen's Group Policy Inheritance tab to link various GPOs in an order that ensures appropriate application of the settings. EC policies that you configure by using the *Security Guide* templates should have a higher precedence than Default policies, and override policies should have higher precedence than the EC policies.

Different policies apply depending on which organizational unit (OU) the server resides in. You can view all the GPOs that apply to an OU (either directly or by inheritance) by selecting the Group Policy Inheritance tab.

A More Secure System

Deploying the *Security Guide* templates requires a lot of planning and a preproduction lab environment where you can test functionality. However, using the security templates in combination with the SCW to create policies for your Windows servers gives you control over your security environment. You'll be able to make changes across many servers, comply with Microsoft's security best practices, and add reliability and stability to your environment. See "Do's and Don'ts of Using Security Templates," page 46, for tips to successfully use the security templates.

If Microsoft wants organizations to take security seriously, Exchange (and other servers and applications) should work out of the box with the EC security templates. At the very least, Microsoft should document the problems that this article identifies. This article summarizes the benefits and problems involved in using the security templates and the SCW; however, it's not a replacement for reading the documentation that comes with the guide.

InstantDoc ID 96177

Russell Smith

(rms@russell-smith.net) is an independent IT consultant who specializes in management and security of Microsoft-based systems. He has served as Active Directory security consultant for the United Kingdom NHS National Programme for Information Technology. He also provides training in the areas of Web authoring (HTML, Dreamweaver, and Flash) and Microsoft Office.

DIG OIT BY DIGGING INTO

Turn complex and repetitive tasks into simple operations

by Robert Sheldon

ILLUSTRATION BY TODD DAVIDSON/IMAGES.COM

As a systems administrator, you're well aware of how busy you are. If you're not putting out four-alarm fires, you're playing catch-up on last month's and maybe even last year's projects. The idea that you can squeeze anything else into your schedule seems as preposterous as Microsoft Bob 5.0. Yet there's one technology that's well worth making time for—Windows PowerShell, an interactive scripting and command-shell environment that lets you automate administrative tasks and access a wide range of information.

With PowerShell, you can run commands directly at the command prompt or run scripts that contain those commands. PowerShell supports its own scripting language, which leverages the Microsoft .NET object model to combine the rich features of object-oriented programming with the ease of command-shell scripting. What that means for you is a powerful environment that can turn complex and repetitive tasks into simple operations. Through PowerShell, you can access a variety of systems and technologies, such as Active Directory (AD) and Windows Management Instrumentation (WMI) to perform such tasks as retrieving event log entries, disabling user accounts in AD, and retrieving a computer's user-defined shares.

POWERSHELL

PowerShell runs on Windows Vista, Windows Server 2003 SP1, Windows Server 2003 Release Candidate 2 (R2), and Windows XP SP2. It will also run on Windows Server 2008 (formerly code-named Longhorn Server). You can install PowerShell on x86, x64, and IA64 processor architectures. However, before you install PowerShell, you must first install Microsoft .NET Framework 2.0. You can download the .NET Framework at http://msdn2.microsoft.com/en-us/netframework/aa569263.aspx and PowerShell at http://www.microsoft.com/technet/scriptcenter/hubs/msh.mspx. To install either product, simply run the setup program and follow the steps in the installation wizard.

After you've installed PowerShell, you're ready to go. Click Start, All Programs, Windows PowerShell 1.0, then Windows PowerShell. In the PowerShell window, you can run commands or PowerShell scripts (.ps1) files by entering the command or filename at the command prompt. To test your installation, type

```
get-help
```

at the command prompt and press Enter. This displays information about getting help in PowerShell—a handy command to be sure. (For more cmdlets that are helpful when learning PowerShell, see the sidebar "PowerShell Pointers.")

You're now ready to run commands and scripts. All you need to do is to learn a little about the PowerShell language. To help you with that, I'll review three sample scripts—RetrieveAppEvents.ps1, DisableUser.ps1, and FindShares.ps1—that demonstrate many of the basic concepts in the language and show you how easy it is to get started with PowerShell.

RetrieveAppEvents.ps1

RetrieveAppEvents.ps1 in Listing 1 retrieves entries from the local application event log and saves them to a text file. As callout A shows, I begin the script by defining the $date variable. A dollar sign always precedes parameter and variable names. The variable uses the Get-Date cmdlet to retrieve the current date and time (aka datetime). A cmdlet, which is similar to a function, performs a specific action and usually takes the form of *verb-noun*. I then use the AddDays method to obtain the datetime exactly 24 hours (i.e., 1 day) prior to the current datetime and assign that value to the $date variable.

Next, I create the FormatEntryType function, as callout B shows. A function is a named block of code that performs a specific action. After you create the function, you can reference it anywhere in your script and the block of code will run. In this case, the FormatEntry function retrieves the content of a text file, modifies that content, and saves it to a second text file. The function takes the $file parameter, which passes the pathname of the target text file into the function.

The first command in the function's statement block (enclosed in curly brackets) uses the Get-Content cmdlet to retrieve content from the text file in $file. Notice that a pipe (|) follows the cmdlet. This indicates that the content should be passed down the pipeline to the next cmdlet. One feature that makes PowerShell so useful is the ease with which you can create pipelines to pass information from one statement to the next.

In this function, I pass the data retrieved by

Listing 1: RetrieveAppEvents.ps1

```
A # Calculate the datetime for one day earlier than the current datetime.
  $date = (get-date).addDays(-1)

B # Create a function to format the entry types.
  function FormatEntryType ($file)
  {
    # Retrieve the content from the AppEvents.txt file.
    # Replace the error and warning entry types.
    # Output the changes to AppEvents_EntryTypes.txt.
    get-content $file |
    foreach-object { $_ -replace "error", "*** ERROR ***" } |
    foreach-object { $_ -replace "warning", "* Warning *" } |
    out-file -filePath c:\scripts\AppEvents_EntryTypes.txt
  }

C # Retrieve the application events for the past day.
  $events = get-eventlog application | where-object `
    {$_.timeGenerated -gt $date}

D # Output the application events to AppEvents.txt. Record only
  # the time of the event, entry type, source, and message.
  $events | foreach-object { out-file -filePath c:\scripts\AppEvents.txt -append `
    -inputObject $_.timeGenerated, $_.entryType, $_.source, $_.message }

E # Run the FormatEntryType function against AppEvents.txt.
  FormatEntryType c:\scripts\AppEvents.txt
```

PowerShell Pointers

PowerShell has many built-in cmdlets that provide information about the language itself. When you're learning PowerShell, you'll likely find the following cmdlets helpful:

Aliases. PowerShell supports aliases that you can use to reference cmdlets. For example, you can use *ForEach* or *%* to reference the ForEach-Object cmdlet. For a list of aliases, enter

```
Get-Alias
```

at the PowerShell command prompt. For general information about aliases, enter

```
Get-Help About_Alias
```

Cmdlets. For a list of cmdlets, enter

```
get-help -category cmdlet
```

To retrieve detailed information about a cmdlet, including the parameters it supports, enter

```
get-help CmdletName -detailed
```

where *CmdletName* is the name of the cmdlet you want to get information about. For example, to retrieve information about the Get-Service cmdlet, enter

```
get-help get-service -detailed
```

ForEach-Object cmdlet versus ForEach statement. The ForEach-Object cmdlet and ForEach statement aren't the same. To learn how they differ, enter

```
Get-Help About_ForEach
```

Help. To retrieve information about how to use PowerShell help, enter

```
Get-help get-help
```

Operators. To learn about operators (e.g., -replace, -gt, -ne), enter

```
Get-Help About_Operator
```

PowerShell security. To learn about PowerShell security, enter

```
Get-Help Set-ExecutionPolicy
```

WMI classes. For information about how to access WMI classes, enter

```
Get-Help Get-WmiObject
```

InstantDoc ID 96275

Get-Content down the pipeline to a ForEach-Object cmdlet, for which you can use the alias ForEach or %. The ForEach cmdlet lets you iterate through objects within a collection. In this case, the collection is made up of the content of the text file. By default, the objects in a file collection are delineated by line breaks, which means the collection contains one object per line. (You can override the default behavior, but for the purposes of this example, line breaks work well.)

The ForEach cmdlet uses an expression, enclosed in curly brackets, to process each object in the collection. The expression begins with the $_ symbol, which refers to the current input object from the collection. The expression then uses the -replace operator to replace any *error* object with an *** *ERROR* *** object. In other words, any line that contains only the word *error* is replaced with *** *ERROR* ***. A second ForEach cmdlet performs a similar operation on *warning* objects.

The second ForEach cmdlet pipes the content to the Out-File cmdlet, which sends the content to the AppEvent_EntryTypes.txt file. Each time you run the function within a script, the content will be inserted into that file.

The code at callout C retrieves the application event entries and assigns the results to the $events variable. To retrieve data from the application events log, I use the Get-Eventlog cmdlet and specify *Application* as a parameter. I then send the event data down the pipeline to the Where-Object cmdlet. The backtick (`) at the end of the line indicates that the statement continues to the next line. However, you don't have to use a backtick when a line breaks at a pipe.

The Where-Object cmdlet filters the data based on the expression defined in the curly brackets. As with ForEach, you use $_ to reference the current object within the collection. In this case, the collection is made up of the event entries. You can also use $_ to reference specific properties within the object. For example, the expression uses $_ to reference the TimeGenerated property. You reference an object's properties by adding a period followed by the property name. The expression then uses the greater than (-gt) operator to compare the TimeGenerated property's value to the value in the $date variable. As a result, the $events variable includes only events generated within the last 24 hours.

Next, I use the $events variable to access the events. The statement in callout D passes the content in $events down the pipeline to a ForEach cmdlet. The ForEach expression consists of a Out-File cmdlet that outputs the event content to AppEvents.txt. The Out-File cmdlet includes the -Append option to ensure that each event is added to the file without overwriting any events. In addition, the cmdlet includes the -InputObject option, which uses the $_ symbol and property names to specify the types of data to save to the file. As a result, the output file includes only the timestamp, entry type, source, and message associated with each event.

Finally, the code in callout E calls the FormatEntryType function and passes the AppEvents.txt file's pathname to the function. As you saw earlier, this function retrieves the data from the first text file, updates the data, and adds it to the AppEvents_EntryTypes.txt file. Figure 1 shows a sample event from AppEvents_EntryTypes.txt.

To run RetrieveAppEvents.ps1 from the PowerShell command prompt, you simply need to type the script's pathname and press Enter. So, the command might look like

```
c:\scripts\retrieveappevents.ps1
```

However, PowerShell prevents you from running scripts by default. To modify the default behavior, you must change the Power-

Thursday, March 15, 2007 6:36:56 AM
*** ERROR ***
Userenv
Windows cannot determine the user or computer name. (The RPC server is unavailable.)
Group Policy processing aborted.

Figure 1: Sample event from AppEvents_EntryTypes.txt

Listing 2: DisableUser.psl

```
(A) # Define the parameter used to pass in the user account name
    # from the command line.
    param ($sam = $(throw "You must include the user account name."))

(B) # Create a searcher object to find the data in AD.
    $ds = new-object directoryServices.directorySearcher

    # Define a filter on the searcher object to retrieve the specified user account.
    $ds.filter = `
      "(&(objectCategory=person)(objectClass=user)(samAccountName=$sam))"

    # Retrieve the user account and assign it to variable.
    $dn = $ds.findOne()

(C) # Retrieve the user account's description and assign it to the $dn variable.
    $desc = $dn.properties.description

    # Retrieve the current datetime and assign it to the $date variable.
    $date = get-date

(D) # Run the If statement if the user account is found.
    if ($dn.path.length -gt 0)
    {
      # Create an ADSI object using the user account's path.
      $user = [ADSI]$dn.path

      # Disable the user account.
      $user.psBase.invokeSet("accountDisabled", $true)

      # Append the user account's description.
      $user.Put("description", "$desc (disabled $date)")

      # Commit the user account changes to AD.
      $user.setInfo()

      # Return a message that says the user account has been disabled.
      write-host "User account" $sam "disabled."

      # Return the user account's DN.
      write-host "Distinguished name:" $dn.properties.distinguishedname
    }

(E) # Run an Else statement if user account isn't found.
    else
      # Return a message that says the user account wasn't found.
     {write-host "User account" $sam "not found."}
```

Listing 3: FindShares.psl

```
A # Define the parameter that passes in the computer name to the script.
  # Use the local computer if no name is specified.
  param ($computer = ".")

B # Create a WMI object to access the Win32_Share class. Pass the
  # data down the pipeline to a filter, which removes the default shares.
  # Then, pass the data down the pipeline to sort the results by name.
  $shares = get-wmiobject -class "Win32_share" `
    -namespace "root\CIMV2" -computername $computer |
    where-object `
    {
      ($_.caption -ne "default share") `
      -and ($_.caption -notlike "remote*") `
      -and ($_.caption -notlike "logon*") `
    } |
    sort-object name

C # Run an If statement if user-defined shares exist.
  if ($shares -ne $null)
  {
    # Add a blank line before the results. Create a
    # ForEach statement to iterate through the shares.
    write-host
    foreach ($share in $shares)
    {
      # For each share, provide the name and path.
      write-host "Share name: " $share.name
      write-host "File path: " $share.path
      write-host
    }
  }

D # Run an Else statement if no user-defined shares exist.
  else
  {
    if ($computer -eq ".")
    {
      # Return a message that names the local computer.
      write-host
      write-host "The computer $env:computerName contains only the default shares."
      write-host
    }

    else
    {
      # Return a message that names the specified computer.
      write-host
      write-host "The computer $computer contains only the default shares."
      write-host
    }
  }
```

Shell security settings. To get started, you can change the settings by entering the command

```
set-executionpolicy remotesigned
```

Thereafter, you can run scripts that you create, but any other script must be digitally signed.

Now that you've seen your first script, you should be familiar with many of the basic PowerShell concepts. As you'll see, a lot of these concepts apply to other scripts.

DisableUser.ps1

DisableUser.ps1 in Listing 2, page 51, disables user accounts in AD. As callout A shows, I begin this script by using the Param keyword to define a parameter ($sam) that passes in the user account that's entered on the command line when the script is run. When using this keyword, you have several options:

- You can use only the Param keyword and the name of the parameter in parentheses.
- You can define a default value in case no value is specified when running the script.
- You can use the Throw keyword (as I've done here) to return an error message when no value is specified. When returning an error message, you must enclose the Throw keyword and message in parentheses and precede the parentheses with a dollar sign.

The code at callout B locates the user account in AD. This code begins by creating an object that searches the directory. To create the object, I use the New-Object cmdlet with the DirectorySearcher class in the DirectoryServices namespace. (For information about the DirectoryServices namespace, go to http://msdn2.microsoft.com/en-us/library/system.directoryservices.aspx.) I then assign the object to the $ds variable.

Next, I create a filter on the $ds object by setting the object's Filter property ($ds.filter). The filter is based on the Active Directory Service Interfaces (ADSI) attributes defined after the equal sign (=). The filter removes all values except those that conform to the attribute definitions. As a result, the filter returns a user account that is part of the person object category and the user object class and that has a SAM name that matches the one specified in the $sam parameter.

After creating the filter, I use the FindOne method of the $ds object ($ds.findOne()) to retrieve the user account. I assign the account to the $dn variable.

The code in callout C defines two variables. The first variable, $desc, stores the user account's description. To retrieve the description, I use the $dn variable to call the account's properties, then call the Description property ($dn.properties.description). The second variable, $date, stores the current datetime, which I obtain with the Get-Date cmdlet. Both these variables are used later in the script to update the user account's description.

The code in callout D disables the user account. The section is encased in an If statement block that runs when the If condition ($dn.path.length –gt 0) evaluates to true. The condition compares the length of the $dn object's Path property to 0. The Path property contains the LDAP location of the user account in AD. When the Path property contains a value, the If statement block runs.

The first command in the If statement block uses the Path property to create an ADSI object for the user account. The ADSI object, which is assigned to the $user variable, is used to access the object's properties and methods, including the AccountDisabled property.

In the next statement, I set the AccountDisabled property to true. Because AccountDisabled is stored in a binary collection in AD, I use the InvokeSet method on the PowerShell base object (psBase) to update the property. The InvokeSet method takes two arguments: the property name (AccountDisabled) and the new value. To set the AccountDisabled property to true, I use the built-in $true variable.

Now I'm ready to update the user account's description. To do so, I call the $user object's Put method, which takes two arguments: the property name (Description) and the value. In this case, the value is made up of a combination of the $desc and $date variables and the word *disabled*. The value takes the original description and appends the word *disabled*

```
Share name:  Bin
File path:  C:\DataFiles\Bin

Share name:  C
File path:  C:\

Share name:  PowerShell Help Files
File path:  C:\WINDOWS\system32\windowspowershell\v1.0

Share name:  Scripts
File path:  C:\Scripts
```

Figure 2: Sample list of shares

followed by the current datetime.

After updating AD information, you must commit the changes, so I call the $user object's SetInfo method. I then display two messages by using the Write-Host cmdlet. The first message says the account has been disabled. The second message displays the account's distinguished name (DN).

The code in callout E highlights the final part of the script, which is an Else statement block. The Else statement runs when the If condition evaluates to false. For this script, the Else statement uses the Write-Host cmdlet to display a message that says the user account wasn't found.

That's all there is to DisableUser.ps1. When you run this script, you must have access to the AD store. I tested this script on a computer running Windows 2003 Enterprise Edition that was configured as a domain controller (DC). I also tested the script on an XP machine against a Windows 2000 DC.

FindShares.ps1

FindShares.ps1, which Listing 3 shows, retrieves a list of the user-defined shares on a computer. Like DisableUser.ps1, FindShares.ps1 begins by defining a parameter. As callout A shows, the $computer parameter passes the computer name to the script when you run it. However, the parameter uses a default value rather than returning an error message when a parameter isn't provided. In this case, the default value is a period, which refers to the local computer.

The code in callout B uses the Get-WmiObject cmdlet to create a WMI object. The cmdlet uses the -Class option to specify the Win32_Share class, the -Namespace option to specify the root\CIMV2 namespace, and the -ComputerName option to specify the computer name in $computer. Of these options, the -Class option is the most important because it determines the type of information you can access through the WMI object.

After accessing the WMI class information, I pass it down the pipeline to a Where-Object cmdlet. The Where-Object expression, enclosed in curly brackets, includes three conditions. The first condition uses the not equal (-ne) operator to compare the Caption property's value to the phrase *default share*. For the condition to evaluate to true, the property's value can't equal the phrase. The second condition uses the -notlike operator to compare the Caption property's value to the *remote** value. Notice the use of the wildcard, which can represent any characters. For the condition to evaluate to true, the Caption property's value can't begin with the word *remote*, but it can end with any characters. The final condition is similar to the second condition, except that the Caption property's value can't begin with the word *logon*.

The Where-Object expression uses the *-and* logical operator to link the three conditions, which means that they all must be true for a share to be included in the list. I pass the filtered list down the pipeline to a Sort-Object cmdlet, which sorts the list of shares based on the Name property (by default, in ascending, or alphabetical, order). I assign the sorted WMI information to the $shares variable.

The code in callout C is an If statement block. The If condition ($shares -ne $null) uses the -ne operator and the $null system variable to specify that the $shares variable can't contain a null value. When the $shares variable's value isn't null (i.e., the If condition evaluates to true), the If statement block runs.

The If statement block begins with the Write-Host cmdlet. Because the cmdlet specifies no content, it simply returns a blank line. This provides extra spacing to better display the information in the PowerShell window.

The next statement is a ForEach statement. The ForEach statement isn't the same as the ForEach-Object cmdlet, even though they perform the same function. Adding to the confusion is the fact that one of the ForEach-Object cmdlet's aliases is ForEach. Here's how you can tell them apart: When ForEach is at the beginning of a command, it's a ForEach statement. When ForEach is within a pipeline, it's a ForEach-Object cmdlet.

The ForEach statement iterates through the objects (i.e., shares) in the $shares collection. The statement defines the $share variable, which refers to the current object. The ForEach expression uses the $share variable to take action on each object. The first command in the ForEach expression is a Write-Host cmdlet that writes the Name property's value to the PowerShell window. The script accesses the name property through the $share variable. The second Write-Host cmdlet writes the Path property's value to the PowerShell window. The final Write-Host cmdlet simply adds a line after each iteration to make it easier to read the list of shares.

When the If condition ($shares -ne $null) evaluates to false, the Else statement block in callout D runs. The Else statement block contains its own If and Else statement blocks. The nested If condition specifies that the computer name must equal a period. When the computer name is a period, Write-Host uses the COMPUTERNAME environmental variable to return the name. Note that to access an environmental variable, you must precede the variable name with $env:. When the computer name isn't a period, Write-Host returns the name stored in $computer.

When you run FindShares.ps1, you'll obtain a list of shares. Figure 2 shows sample output from this script.

Only Scratching the Surface

As you can see, with PowerShell, you have a lot of flexibility in the type of information that you can access and what you can do with that information. These three examples of how to use PowerShell only scratch the surface. The more effort you devote to learning PowerShell, the greater your payoff will be. And who knows, with these new skills, you might have time to complete last year's projects.

InstantDoc ID 96075

Robert Sheldon

(contact@rhsheldon.com) is a technical consultant and the author of numerous books, articles, and training material related to Microsoft Windows, various relational database management systems (including SQL Server), and business intelligence design and implementation. He is also the author of the novel *Dancing the River Lightly*.

... Tired of Nursing Your Exchange Server?

#1 BEST SELLER!

Anyone who has given birth to an Exchange network knows it can get sick and needs some nursing to stay healthy. In fact, 72% of Exchange Administrators surveyed* have "experienced" an Exchange disaster (feels like the flu)—usually from improper feeding and care.

Like many databases, constant adding and deleting can corrupt an Exchange data file so it eventually turns sour. Replicating, archiving and backing up the data doesn't stop the stink—it just stores it. You've got to…

Fix the Problem

You may have tried the free utilities to fix Exchange. While they help, they are too tedious, time consuming and lightweight to keep your Exchange baby healthy. You've tried the milk, now try some meat!

Pamper Yourself with GOexchange

It's time to try GOexchange, from Lucid8, the #1 best-selling automated disaster prevention and optimization software for Microsoft Exchange 5.5, 2000, 2003 and 2007. As the mother of all Exchange tools, GOexchange helps prevent disasters, repair problems, improves performance, and saves you a lot of time.

> ***"Without routine maintenance, decreasing performance, increased warnings and errors accumulate and database fragmentation transpires, leading to Exchange disasters."***
>
> **Gartner**

Prevent Hiccups

GOexchange removes errors, warnings and inconsistencies within the database—before major corruption makes the database fail.

"GOexchange corrected 2,264 errors and 26 warnings."

Paul Ramos, Director IT

Run, Don't Crawl

In addition to fixing the database, GOexchange removes sluggishness and improves performance by re-indexing and defragmenting the database to permanently remove white space and deleted items. The end result is increased performance and stability with a compact efficient database that's 31 to 55% smaller! Combine this with archiving and the database is up to 91% smaller—making it much quicker to backup.

"..our information stores were reduced by 45-50%."

Dale Huitt, Systems Lead

Automated Babysitter

First, GOexchange is easy to setup and use. Twenty minutes—that's all it takes to get your server up and running. Just schedule it, and walk away!

The software notifies the users, validates the database, runs the backup, conducts a comprehensive system analysis and diagnostics, logs the errors, and notifies you if it discovers a "stop" error—then it repairs and defragments the database, generates a thorough report and schedules the next event.

You can do some of this work yourself, but why waste time doing repetitive maintenance, when GOexchange can do it for you—faster and more effectively than doing it by hand.

Created By

Lucid

Solutions Inspiring Confidence

"Life before GOexchange…was an absolute nightmare, late nights, long weekends and upset users."

Marty Grogan, CTO

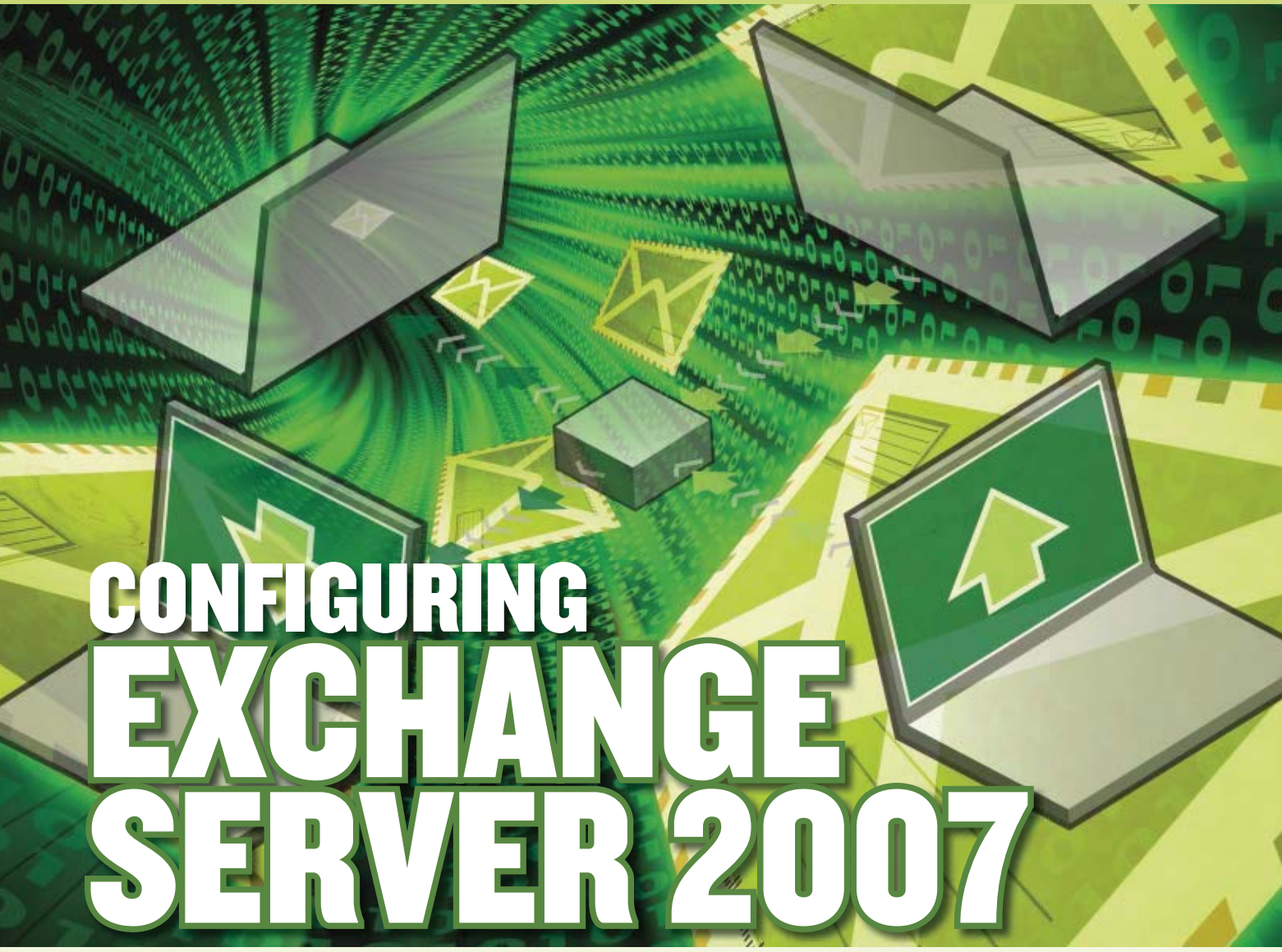
Stop The Crying

Why not call now, or visit our resource site and learn how to reduce the risk, and avoid the pain. Protect your exchange data, maximize performance, and spend a weekend at home—*instead of babysitting Exchange.*

Special Offer

- Free Software for analysis of your Exchange server!
- Free White Paper—"Basic Feeding of Your Exchange Server."
- View the Gartner webcast: "Protecting Microsoft Exchange…"

Go to: www.Lucid8.com/GoITPro
Call 425.456.8474
E-mail: Sales@Lucid8.com



CONFIGURING EXCHANGE SERVER 2007

You've installed the new software—here's what to do next

Brien Posey
(http://www.brienposey.com) is the vice president of research for Relevant Technologies. He writes technical content for a variety of publications and Web sites.

After you install Microsoft Exchange Server 2007, you still have a lot of configuration to do before the server is completely functional. Configuration tasks vary considerably depending on the existing Exchange Server organization (e.g., how many servers you have, what jobs those servers are performing) and on the roles installed on the server. Rather than discussing every potential configuration setting, I'll instead focus on general configuration tasks and the initial configuration of the Mailbox, Client Access, and Hub Transport server roles because they're the most commonly used. For a checklist of the tasks, see the sidebar, "Server Configuration Steps for Exchange 2007," page 59.

General Configuration Tasks

One aspect of Exchange 2007 that's particularly useful is that you don't have to guess about which configuration tasks to perform after installation. You can easily find a list of post-installation deployment tasks by opening Exchange Management Console and clicking the Microsoft Exchange container, which displays the Exchange Server 2007 Finalize Deployment page. As Figure 1, page 56, shows, most of these tasks are organized by server role. However, the first two tasks on the list apply to all Exchange 2007 servers, regardless of the roles they're hosting.

Enter a product key. Although the first configuration task listed for all Exchange 2007 servers is entering a product key, I recommend saving this task for later. Exchange 2007 will run in a fully functional state without a product key

Figure 1: Viewing configuration tasks in Exchange Management Console

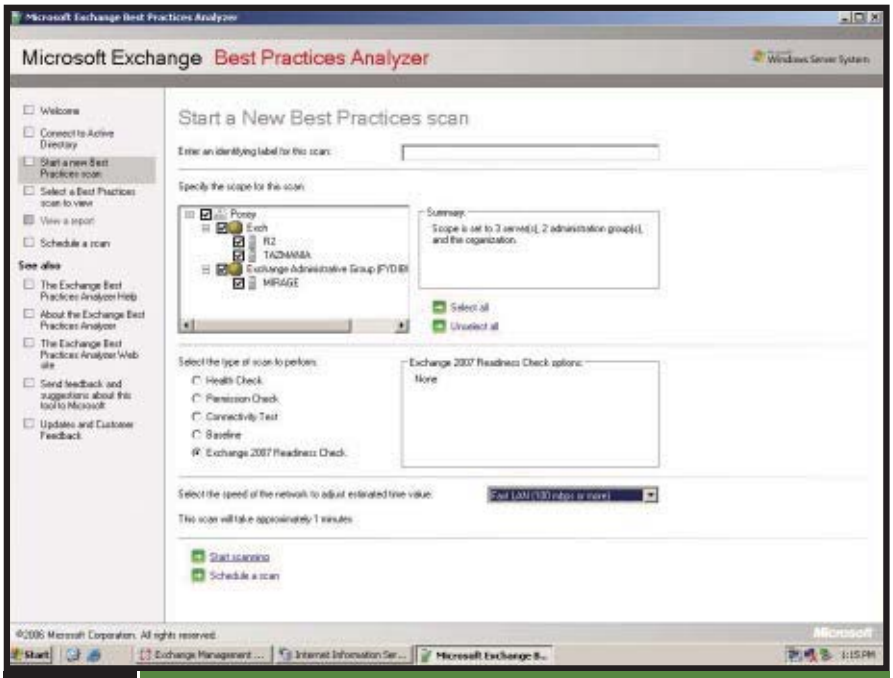


Figure 2: Performing an Exchange 2007 readiness check in ExBPA

for 120 days. Each time you open Exchange Management Console, Exchange tells you how many days you have until a product key is required. Microsoft products typically can be activated only a certain number of times; Exchange 2007 doesn't use a true activation, but it does use a similar online validation. Waiting to enter a product key lets you work out any kinks in your system without wasting your validations should you need to reinstall Exchange a few times or if you decide to run Exchange on different hardware.

Run the Best Practices Analyzer. The next task on the list is to run the Exchange Server Best Practices Analyzer (ExBPA), a tool that helps you make sure your Exchange server is configured for optimum performance and security. ExBPA is included in Exchange 2007, but you can also download it separately from Microsoft's Web site (http://www.microsoft.com/downloads/details.aspx?FamilyID=dbab201f-4bee-4943-ac22-e2ddbd258df3). As Figure 2 shows, ExBPA even lets you perform an Exchange 2007 readiness check on your existing organization and network infrastructure before installation.

It's a good idea to run ExBPA immediately after installation as Microsoft recommends. ExBPA's report might point out more inadequacies than you'd care to see, but this is partially because the server hasn't been fully configured yet. You can use the report to help you with the configuration process. To learn more about how ExBPA can assist in your Exchange configuration, see "ExBPA: Analyze This!" January 2005, InstantDoc ID 44709, and the *Exchange & Outlook Administrator* article "The Exchange Best Practices Analyzer," February 2005, InstantDoc ID 44793. After you've finished configuring the server, you can run ExBPA again to see whether you've caught all the problems.

Configuring the Mailbox Server

The first task for the Mailbox server is configuring Offline Address Book (OAB) distribution for Microsoft Office Outlook 2007 clients. Because you can host an OAB on a Client Access server, which is accessible from the Web, the OAB can be distributed to any Outlook 2007 client with an Internet connection.

Assuming you have a Client Access server in your organization, you enable Web distribution of the OAB by navigating through the Exchange Management Console tree to Organization Configuration\Mailbox. Click the Mailbox container, then click the Offline Address Book tab in the detail pane to display a link for the default OAB. Right-click the link and choose Properties from the shortcut menu. In the Properties sheet, click the Distribution tab, then select the *Enable Web-based distribution* check box. Click the Add button, then select an OAB virtual directory. An OAB virtual directory is created automatically when you deploy your Client Access server.

The last step in the process is to associate a URL with the OAB virtual directory so that Outlook 2007 clients can access the OAB. Navigate through the console tree to Server Configuration\Client Access. When you click the Client Access container, the detail pane displays a list

Figure 3: Configuring the Offline Address Book for legacy clients

of Client Access servers. Select the server that's hosting the OAB virtual directory, and the bottom half of the detail pane displays several tabs for this server. Select the Offline Address Book Distribution tab, and you should see a listing for the OAB URL. Right-click the URL and choose Properties from the shortcut menu. In the OAB Properties sheet, click the URLs tab, which will already contain an internal URL. You'll need to enter an external URL that Outlook 2007 clients can use to access the OAB.

Clients running Microsoft Office Outlook 2003 and earlier will be unable to access the OAB using a Web link. For these clients, you'll have to create a public folder in which to host the OAB. I'm assuming that your server already contains a public folder store; if it doesn't and you don't know how to create one, then you can click the *Configure Offline Address Book (OAB) distribution for Outlook 2003 and earlier clients* link in the tasks list for instructions.

Next, navigate through the console tree to Organization Configuration\Mailbox, then select the Offline Address Book tab in the detail pane. Right-click the Default Offline Address List and choose Properties from the shortcut menu. In the Default Offline Address List Properties sheet, click the Distribution tab. As Figure 3 shows, you must select which legacy clients you want to support, then select the *Enable public folder distribution* check box.

Configuring the Client Access Server

The Client Access portion of the post-installation tasks list includes two tasks: configuring Secure Sockets Layer (SSL) encryption and configuring Exchange ActiveSync (EAS). However, depending on how your Exchange organization is configured, these tasks might not be necessary.

Configuring SSL Encryption. An SSL certificate is required for encryption when a Microsoft Outlook Web Access (OWA) client connects to the Client Access server. The only time an SSL certificate wouldn't be required on a Client Access server is when you offload SSL encryption to another device to conserve resources on your Exchange server.

The good news is that Exchange 2007 is flexible in the types of certificates it lets you use. You can use an Exchange 2007 self-signed certificate, purchase an SSL certificate from a Certificate Authority (CA), or get a certificate from a public key infrastructure (PKI) CA. The advantage of using a self-signed certificate is that it's free and easy to deploy. However, no one outside your organization will acknowledge the self-signed certificate as having come from a credible source. A certificate from a commercial CA caries credibility but can be expensive to purchase.

To use a self-signed certificate, you generate the certificate by using the Exchange Management Shell's New-ExchangeCertificate cmdlet, as follows:

Figure 4: Using the New-ExchangeCertificate cmdlet to request a certificate

```
New-ExchangeCertificate -GenerateRequest `
  -domainname <yourdomain.com> `
  -FriendlyName <yourdomain.com> `
  -privatekeyexportable:$true `
  -path c:\cert_myserver.txt
```

In the previous command, you'd replace *yourdomain.com* with the name of your domain.

Your configuration tasks will vary depending on your servers' roles and on your Exchange organization's existing configuration.

You can enter multiple domains separated by commas if you want. FriendlyName is the name that's displayed for the certificate being generated; it must be fewer than 64 characters. Figure 4, page 57, shows an example of this command and its output.

Regardless of how you obtain an SSL certificate, the procedure for installing the certificate is basically the same. Open Exchange Management Shell and enter the following command, where *c:\newcert.cer* is the path and filename for the certificate you're importing:

```
Import-ExchangeCertificate `
  -path c:\newcert.cer
```

Now, copy a digest, or thumbprint, of the certificate data to the Clipboard by using the following command:

```
Dir cert\LocalMachine\My |fl
```

If multiple certificates are displayed, select the appropriate certificate by its friendly name. Next, use the information from the Clipboard to enable the certificate on the default Web site by using the following command:

```
Enable-ExchangeCertificate -thumbprint `
  <the value stored in the Clipboard> `
  -services "IIS,IMAP,POP"
```

The last step in the process is to verify that Microsoft IIS is configured to require SSL encryption for virtual directories. Choose Internet Information Services (IIS) Manager from the Administrative Tools menu. In the IIS Manager console tree, navigate to your Default Web site and expand the container to reveal a list of the virtual directories in the default Web site. For each of these directories, right-click the directory and choose Properties from the shortcut menu. In the Properties sheet, click the Directory Security tab, then click Edit in the Secure Communications section to display the Secure Communications dialog box. Select the Require Secure Channel check box and the Require 128-Bit Encryption check box. Click OK twice and move on to the next virtual directory. When you're done, you'll need to restart the POP3 and IMAP services.

Configuring EAS. You'll need to configure EAS only if some users in your organization use mobile devices to send and receive email. For this article, I'll assume that all your mobile users have devices running Windows Mobile 5.0; older versions aren't supported.

First, create a new EAS mailbox policy. Navigate through Exchange Management Console to Organization Configuration\Client Access. Now, click the New Exchange ActiveSync Mailbox Policy link in the Actions pane. Exchange Management Console opens a screen that lets you enter the particulars for your mailbox policy. As Figure 5 shows, you must enter a name for the policy you're creating, and you can set a number of security requirements, most of which are related to the device's password. Select the requirements appropriate for your organization, then click New to create the policy.

Keep in mind that merely creating a policy doesn't activate it; an EAS policy must be assigned to one or more mailboxes to be effective. Therefore, you can create multiple EAS policies and assign different policies to different users.

To assign an EAS policy to a mailbox, click the Exchange Management Console's Recipient Configuration container to display a list of all the mailboxes in the Exchange organization. Display the Properties sheet for the mailbox you want to apply the policy to and click the Mailbox Features tab. Choose the Exchange ActiveSync option from the list of mailbox features, then click Properties to display the Exchange ActiveSync Properties dialog box. Select the Apply an Exchange ActiveSync Mailbox Policy check box, then click Browse to locate and select the policy you want. Click OK twice to associate the policy with the mailbox.

Figure 5: Setting security settings for an EAS policy

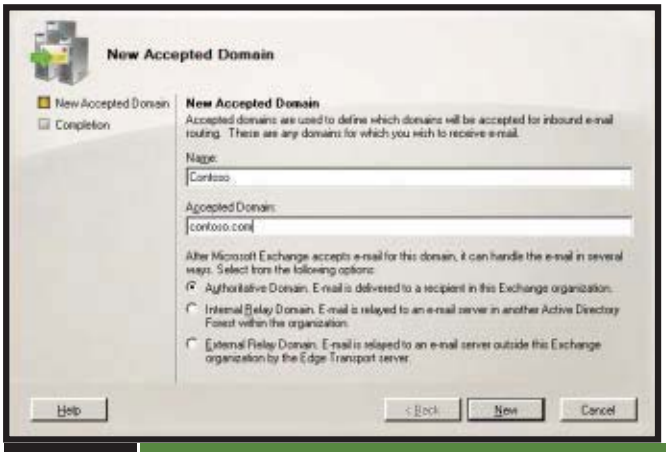


Figure 6: Configuring a new email domain in Exchange

Configuring the Hub Transport Server

You might need to perform as many as three post-installation tasks on servers hosting the Hub Transport role: configuring the domains for which you'll accept email, subscribing to an Edge Transport server, and creating a postmaster mailbox. Depending on the specifics of your Exchange organization, any or all of these tasks might be optional.

Configuring the domains for which you'll accept email. Your Exchange server will be configured automatically to accept mail for your forest root domain, but you might need to configure it to accept mail from external SMTP domains as well. For example, my network is divided into two domains: production.com and test.com. My Exchange server was configured by default to accept mail for production.com, but my email comes through an external domain, brienposey.com. I therefore had to configure my Exchange server to accept mail from this external domain.

To add a domain, navigate through the console tree to Organization Configuration\Hub Transport. Click the Hub Transport container, click the Accepted Domains tab in the detail pane, then click the New Accepted Domain link in the Actions pane to add the domain to the list. As Figure 6 shows, you need to enter the domain's Fully Qualified Domain Name (FQDN) and a display name. You must also specify whether the domain is authoritative, an internal relay domain, or an external relay domain. Click New, and the domain will be added to the list.

Subscribing the Edge Transport server. Setting up an Edge Subscription is required only if your organization uses an Edge Transport server. An Edge Subscription is basically a one-way trust with the Active Directory (AD) database that lets the Edge Transport server receive AD information without compromising the AD database in the process. First, you create an XML file on the Edge Transport server by using the New-EdgeSubscription cmdlet. Then, copy the XML file to your Hub Transport server. For security reasons, be sure to erase the file from the Edge Transport server. Navigate through the console to Hub Transport, click the Edge Subscription tab, then click the New Edge Subscription link in the Actions pane. Now, click Browse to locate the XML file, verify that the *Automatically create a Send connector for this Edge Subscription* check box is selected, then click New to import the XML file and create the Edge Subscription. For more detailed instructions for configuring an Edge Subscription, click the Subscribe Edge Transport Server link in the list of post-installation configuration tasks.

Creating a Postmaster Mailbox. The last step in the configuration process is to configure a mailbox to act as the postmaster. If there are other Exchange servers in your organization, this step might not be necessary, but you need to be sure. Open Exchange Management Shell and enter the following command:

```
Get-TransportServer
```

Look at the ExternalPostmasterAddress column in the results and verify that an address for the postmaster exists. If an address doesn't exist, you'll need to specify a postmaster address by entering the following command:

```
Set-TransportServer -<server name> `
  -ExternalPostmasterAddress `
    <postmaster email address>
```

As you can see, this command requires you to enter a server name and the email address for the postmaster account. You can create a dedicated mailbox to act as a postmaster mailbox, or you can send postmaster messages to a user who already has a mailbox.

Finishing What You Start

As you can see, installing Exchange 2007 is only half the fun. You'll still need to complete these important configuration tasks before you can use your Exchange 2007 server. Keep in mind that your actual configuration tasks will vary depending on your servers' roles and on your Exchange organization's existing configuration. The post-installation tasks list in Exchange Management Console should help you finish what you started and get your servers ready to run.

InstantDoc ID 96044

SERVER CONFIGURATION STEPS FOR EXCHANGE 2007

You've installed Exchange Server 2007, but what do you do next? You still need to configure your servers. Fortunately, the Exchange Server 2007 Finalize Deployment page in Exchange Management Console walks you through the tasks you need to perform. Here are the steps you might still need to take:

Step 1: Complete Tasks that Apply to All Servers

You need to enter a product key, though Microsoft gives you a 120-day grace period to do so. You should also run Exchanger Server Best Practices Analyzer (ExBPA) to help you optimize performance and security.

Step 2: Configure the Mailbox Server

You need to configure Offline Address Book (OAB) distribution for Microsoft Office Outlook 2007 clients. For clients running Microsoft Office Outlook 2003 and earlier, you need to create a public folder to host the OAB.

Step 3: Configure the Client Access Server

Two tasks might be necessary to configure your Client Access server. First, you need to configure Secure Sockets Layer (SSL) encryption for Microsoft Outlook Web Access (OWA) client connections to the Client Access server. Second, you need to configure Exchange ActiveSync (EAS) if some of your users send and receive email from mobile devices.

Step 4: Configure the Hub Transport Server

Your Exchange server will be configured automatically to accept mail for your forest root domain, but you might need to configure it to accept mail from external SMTP domains as well. If you're using an Edge Transport server, you need to set up an Edge Transport subscription. Also, you need to make sure you've configured a mailbox to act as the postmaster.

InstantDoc ID 96045

SHAREPOINT & OFFICE PRO

SHAREPOINT FEATURE

How SharePoint Matches Up to Public Folders

Learn about SharePoint to help you assess a potential transition

by Emer McKenna

It's not too early to prepare for retirement—of public folders, that is. Eventually public folders will no longer be in Microsoft Exchange. In September 2006, Gartner Research published a report recommending that organizations prepare to migrate away from public folders (http://download.microsoft.com/download/6/D/A/6DA5F58F-5146-4897-8111-DF32896FC1B7/Rapport_Gartner.pdf). But never fear: SharePoint's Microsoft Outlook and Exchange integration features enable administrators to begin the transition away from public folders to using SharePoint as an alternative repository for shared information. In fact, Microsoft has already begun to emphasize SharePoint as its collaboration platform to replace public folders. Although SharePoint isn't a perfect replacement for public folders at all sites, it can ease the transition away from public folders.

Let's peruse some popular public folder features and how they map to the latest SharePoint technology. Some features apply to both Windows SharePoint Services 3.0 (WSS 3.0—a component of Windows Server 2003, providing core SharePoint functionality) and Microsoft Office SharePoint Server 2007 (MOSS 2007—which adds enriched functionality such as enterprise content management); other features apply to MOSS 2007 only.

Outlook Integration

Outlook is for many the primary interface for business communications, and the accessibility of public folders from Outlook has been fundamental to their adoption.

Outlook synchronizes public folder content to the offline folder store (OST), to let users work with mailbox and public folder data while offline. WSS 3.0 provides integration with the Microsoft Office 2007 suite, the Microsoft Office 2003 suite, and Outlook in particular. You can connect SharePoint calendars and contact lists to Microsoft Office Outlook 2003. If you're using Microsoft Office Outlook 2007, you can also connect SharePoint task lists, discussion boards, and document libraries. Other SharePoint items, such as custom lists, custom views, and custom properties are not yet supported.

To connect a SharePoint container to Outlook, use your browser to navigate to the container and select *Connect to Outlook* from the Action menu.

The first time you connect a SharePoint container to Outlook, Outlook creates a PST file in your Windows profile. The file is named SharePoint Folders.pst for Outlook 2003 and SharePoint Lists.pst for Outlook 2007. A folder is created in the PST file that represents the connected container. Subsequent container connections are represented as additional folders in the PST. Outlook uses its Send/Receive functionality to synchronize content between SharePoint and Outlook. Outlook 2003 provides one-way offline synchronization (SharePoint to Outlook) for calendars and contact lists. Outlook 2007 extends this integration providing two-way offline synchronization for calendars, contacts,

Learning Path

***WINDOWS IT PRO* RESOURCES:**

To learn more about how public folders map to previous versions of SharePoint:

- "Migrating Public Folders from Exchange to SharePoint," InstantDoc ID 50172
- "SharePoint and Public Folders, Part I," InstantDoc ID 92930
- "SharePoint and Public Folders, Part 2: Migration Options," InstantDoc ID 93127
- "SharePoint Integration with Outlook 2007, Part I," InstantDoc ID 95919

tasks, and discussion lists and one-way synchronization (SharePoint to Outlook) for SharePoint document libraries. Although you might not want to move completely over to SharePoint until its offline synchronization improves, if you're using public folders for collaborating on documents, SharePoint is actually a better environment in spite of the one-way synchronization limit.

You can use Office 2007's Edit Offline function to perform manual synchronization of Office documents stored in document libraries. Outlook 2007 keeps track of documents in the SharePoint PST that were modified while you were offline. Office 2007 adds a link to each modified document to the Offline Documents search folder in the PST, providing a single location to track all offline changes. After you're back online, you can open each modified document and save your changes back to the SharePoint server. Office 2007 handles any version conflicts.

Other Office 2007 products such as Microsoft Office Groove 2007 and Microsoft Office Access 2007 provide capabilities such as two-way synchronization between document libraries and custom lists, respectively. (For more information about synchronizing data by using Groove, see the Microsoft Virtual Lab at http://msevents.microsoft.com/cui/webcasteventdetails.aspx?eventid=1032326933&eventcategory=3&culture=en-us&countrycode=us; for more information about synchronizing data between SharePoint and Access, see the Microsoft article "Introduction to integrating data between Access and a SharePoint site" at http://office.microsoft.com/en-us/access/ha101314631033.aspx.) Additionally, third-party products such as Colligo Contributor for SharePoint, from Colligo Networks, provide two-way synchronization of lists, document libraries, and form libraries, including all associated properties and views.

Discussion-Group Integration

You can use Exchange public folders to archive group discussions. Public folders have an associated email address that lets an administrator make the public folder a member of a Distribution Group (DG). All messages sent to the DG are posted to the associated public folder, effectively creating an archive of the discussions emailed to the group. The public folder permissions must allow group members to create new content in the folder; otherwise, attempts to post to the folder will fail.

To replace the public folder functionality, you can create a group in SharePoint that maps to a DG in Active Directory (AD) and to a discussion board in SharePoint. The members added to the SharePoint group are automatically added to the associated DG in AD. The AD DG appears in the Global Address List (GAL), and any messages sent to it are sent to all the DG members and posted to the SharePoint discussion board. The discussion board permissions have to allow DG members to contribute content to the board. The discussion board honors threading from replies, and each post in the archive contains a history of the conversation thread.

This approach is analogous to the public folder approach, especially as you can synchronize the list to Outlook and it's accessible from a Web browser, although the archives go to a different place for the user. Another added benefit is the fact that SharePoint automatically indexes the content stored in the archive and thus the discussions are accessible through the SharePoint Search UI.

An administrator can configure the SharePoint farm to allow incoming email, which means that document libraries, form libraries, and lists can receive content via email messages. When you configure a list or document library to accept incoming email, you can specify whether to retain the original message or only the attachments. If more than one document is attached to the message, SharePoint posts each attachment as an individual item in the document library.

When enabling a SharePoint container to accept email, the user identifies an email address for the container. If the SharePoint Directory Management Service is enabled, a matching contact object is automatically created in the appropriate organizational unit (OU) in AD. Unfortunately, in Microsoft Exchange Server 2003 and Exchange 2000 Server environments, the Directory Management Service doesn't populate all the required attributes for a mail-enabled contact object, causing attachments mailed to the container to be dropped. For more information about dropped email attachments, see "Attachment is missing from an email message that is sent to a Microsoft Windows SharePoint Services 3.0 document library" (http://support.microsoft.com/kb/926891).

Other anomalies exist on the Exchange Server 2007 side in regard to mail-enabled contact creation. For example, although the Directory Management Service relies on the recipient update service to stamp the proxyAddresses attribute, Exchange Server 2007 doesn't which means that objects provisioned by using the Directory Management Service will be incomplete.

Multiple Content Types

Public folders let users store multiple content types in the same folder hierarchy and, in some cases, the same folder. For example, a team can share a set of public folders that store the team calendar, contacts, and project information. The project folder could contain Microsoft Office Project documents, Microsoft Word documents, Microsoft Excel spreadsheets, and email messages. However, public folders are limited in that certain disparate message classes—such as an appointment, a contact, and a mail message—cannot coexist in a single folder.

WSS 3.0 introduces the concept of content types. A content type describes the characteristics of an item in SharePoint, including its properties, workflows, associated document template, and information management policies. For example, you can define a budget content type that has a budget template, a specific set of custom properties, and an approval workflow associated with it. When a user creates an item of that budget content type, he or she creates a budget document from the template, populates the required properties, and saves the document, triggering an approval workflow. SharePoint supports the storage of multiple content types within the same container. SharePoint content types are managed and updated from a central location and can be deployed across an organization to quickly roll out updates to forms or document templates.

The content types assigned to a SharePoint container are available from the container's main menu, making it easy for a user to create an item of a specific type. Together, SharePoint's content-type functionality and the ability to email-enable

Empower Your People to Accelerate Business Value – with CorasWorks® on SharePoint

More than 750,000 Users Have Been Empowered Thanks to CorasWorks' Workplace Software.

CorasWorks takes the technical work, and the costs, out of creating a powerful, customized, web-based workplace of integrated applications on SharePoint (2003 and 2007). With CorasWorks, designing and building business solutions on SharePoint can be done quickly, easily, and cost-effectively. IT users can save time and money, while reducing their application backlog. Business users, who know best what they need to succeed, can create and enhance their own business applications.

CorasWorks Accelerates Business Value with Microsoft® SharePoint®

Experience how easy and powerful it can be with CorasWorks:
Go hands-on and start creating and integrating applications – without programming!
CorasWorks offers free, 1-Day, Hands-on, Workplace Workshops in a city near you.

Register Today at www.corasworks.net/SharePoint or call 1-866-580-3115!

CORASWORKS®

www.corasworks.net

SharePoint containers provide a repository from which you can initiate a specific workflow or information management policy.

Security

From Outlook, the public folder owner can apply role-based permissions to public folders, granting read, write, and delete access. Using the Exchange Folder Visible permission, you can specify which users see the presence of the folder. This is an important feature from a usability standpoint: It's frustrating to click a folder only to receive an access denied message. Public folder permissions are set on a folder level. If users have access to a folder, they automatically have access to all nonfolder items within that folder. This is where SharePoint has an advantage over Exchange—you can apply role-based security at the item level, letting users see only the items to which they have access, as Figure 1 shows. Although Exchange public folder permissions don't map to SharePoint permissions, you can use the same AD mail-enabled security groups to apply security to both environments. Surprisingly, SharePoint lacks the ability to restrict the creation of subfolders, a security feature many organizations would like to have, and which public folders do offer.

Document Repository

Public folders are a convenient way to share documents that don't change. But because they lack document management functionality, such as version control and conflict resolution, public folders aren't well suited to sharing dynamic content often generated by team collaboration.

WSS 3.0 provides basic document management features, such as major and minor versioning, check-in/check-out, document profiles, workflow, and auditing. MOSS 2007 adds an additional layer of document management capabilities by providing features such as Web content management and publishing, records management, and policy management.

Deleted-Item Retention

If you delete a public folder item, and you have full read, write, and delete permissions on the folder, you can use Exchange's deleted item retention feature to recover the content. You configure the Exchange server for deleted item retention, including the length of the retention period, which is when item recovery has to occur.

WSS 3.0 has a two-stage recycle bin, which Figure 2 shows. Each site within a site collection has a recycle bin that's accessible to end users. When users navigate to the site recycle bin, they receive a personalized view of the content they've deleted from the site, referred to as the end-user recycle bin, from which they can recover their deleted content. The second level of deleted-item retention occurs at the site-collection level; the administrator has access to this site-collection recycle bin. This bin tracks content deleted from all sites within the site collection, including content currently listed in the end-user recycle bins. When a user empties the end-user recycle bin, the deleted content disappears from that bin but remains in the site-collection recycle bin. The administrator can change the view of the site-collection recycle bin to display only items that have been deleted from the end-user recycle bin, providing a convenient way to retrieve content for a user. The retention period for items in the recycle bin defaults to 30 days; the administrator can also configure this value.

Extensibility

Some companies have embraced the extensibility of public folders by building applications that leverage custom forms, event sinks, and the workflow engine. Exchange provides the ability to create a custom form and associate it with a public folder. Exchange Web forms, available in Exchange 2003 and Exchange 2000, provide a mechanism for building custom Web pages that override the default Microsoft Outlook Web Access (OWA) public folder rendering, in case you want a custom version for your users. However, Exchange Web Forms have been removed from Exchange 2007. If you require this capability, Microsoft recommends that you use ASP.NET to extract data from Exchange 2007 and render it for Web-based clients.

Exchange 2003 and Exchange 2000 support an event architecture that lets your code trigger when items are saved, modified, deleted, moved, or copied within the Information Store (IS). For example, to send an email notification when a user posts a document to a public folder, you register your code in the public folder to be executed when a save event occurs. Exchange supports synchronous and asynchronous events. Synchronous events let you modify an item before a specific action, such as save or delete, is completed. Asynchronous events let you modify an item after the action is completed.

Exchange 2003 and Exchange 2000 provide a workflow engine that uses event sinks to determine the state of an item involved in a workflow process. Additionally, Exchange 2003 and Exchange 2000 include a scripting technology, Collaboration Data Objects for Workflow (CDOWF), which provides tools for writing and managing Exchange workflows.

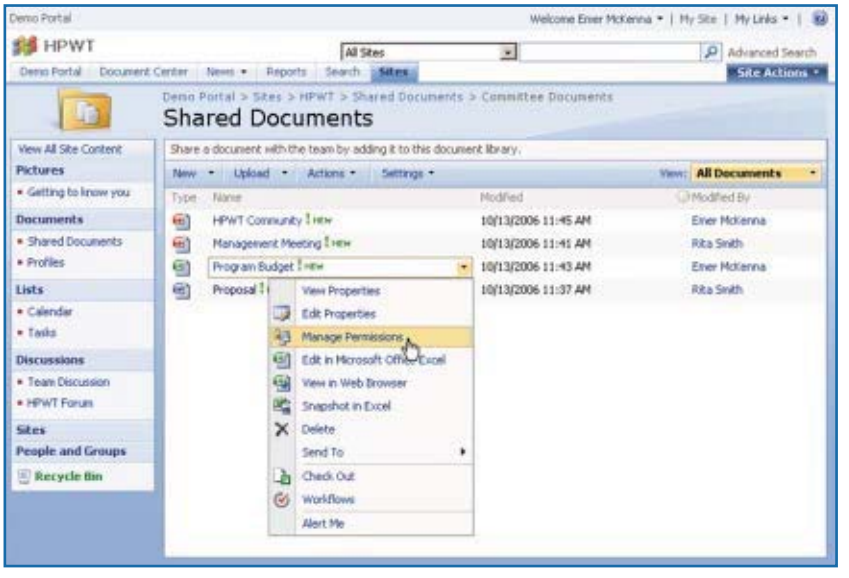


Figure 1: *Applying role-based security at the item level in SharePoint*

However, Exchange 2007 doesn't ship with a workflow engine or CDOWF. Microsoft recommends that existing applications based on public folders be left in place on Exchange 2003 servers. Customers who want to migrate their servers to Exchange 2007 should consider porting their Exchange workflow applications to Windows Workflow Foundation. Workflow Foundation is part of Microsoft .NET Framework 3.0 and will be included in Windows Server 2008 (formerly code-named Longhorn Server). Workflow Foundation provides a runtime engine, a base activity library, and designing tools that run in Microsoft Visual Studio 2005. Companies that have used the more complex features of Exchange and built sophisticated public folder applications should scrutinize the WSS 3.0 and MOSS 2007 feature set to determine whether migration is even an option.

MOSS 2007 offers InfoPath Forms Services, which lets you build XML-based forms and integrate them into your business processes. InfoPath Forms Services provides a server-based runtime environment for Microsoft Office InfoPath 2007 Forms and lets users complete Web-enabled forms by using a browser or an HTML-enabled mobile device. Web-enabled forms remove the requirement for the user to install client components in order to update forms.

SharePoint provides a set of synchronous and asynchronous events that you can integrate with lists, document libraries, sites, and even user operations. Workflow Foundation is at the heart of the MOSS 2007 workflow functionality. MOSS 2007 comes with a set of predefined workflow templates for common workflows, such as approval routing and issue tracking. MOSS 2007 workflows can be associated with a document library, list, or content type and can be authored by using the browser, Microsoft Office SharePoint Designer, or VS 2005 and Workflow Foundation. Additionally, MOSS 2007 workflows can leverage InfoPath forms and support Office 2007 client integration, letting you approve a workflow within an Office application such as Outlook.

Replication

One final important feature of public folders is replication, the transfer of data from one public folder server to one or more public folder servers that maintain replicas of designated folders via a series of content-replication messages. The messages keep the source and destination servers synchronized. Replication moves public folder data closer to the end user to improve performance and is valuable where network latency is a problem. Public folder replication is also commonly used to provide redundancy, so that if an outage occurs on one public folder server, the content remains accessible via a replica on another public folder server.

MOSS 2007 doesn't have out-of-the-box replication functionality; however, third-party vendors such as iOra offer products that fit this scenario. iOra Accelerator for SharePoint replicates Web- and file-based content to a remote server or an end user's machine.

The Way Forward

You can begin to prepare for the retirement of public folders by assessing how public folders are used in your organization. Questions to answer include the following:

- How many folders are actively being used?
- How many folders are dormant?
- Which folders are mail-enabled?
- What is the security structure of your folder hierarchy?
- Are you replicating folders, and why?
- Where are you using custom forms, event sinks, and workflow?

Several tools help with assessment and migration. Quest Software's MessageStats can help you analyze your public folder infrastructure, and its Public Folder Migrator for SharePoint can help you migrate content from public folders to SharePoint containers. AvePoint's DocAve 4.1 Migrator for SharePoint is another such tool.

If you use public folders as a simple document repository and don't rely on replication, migrating to SharePoint is a natural and relatively straightforward process. If, however, you use public folders as a document repository with highly complex workflow, custom forms, and event sink routines, Microsoft recommends that you leave them running happily in Exchange. But given that the future of public folders is uncertain, now would be a good time to start investigating redesigning these applications for a more suitable platform such as Microsoft .NET Framework 3.0, taking advantage of WSS 3.0, MOSS 2007, and Exchange 2007 Web Services. Migrating from public folders provides the opportunity for you to assess these new capabilities and determine whether your organization can leverage them.

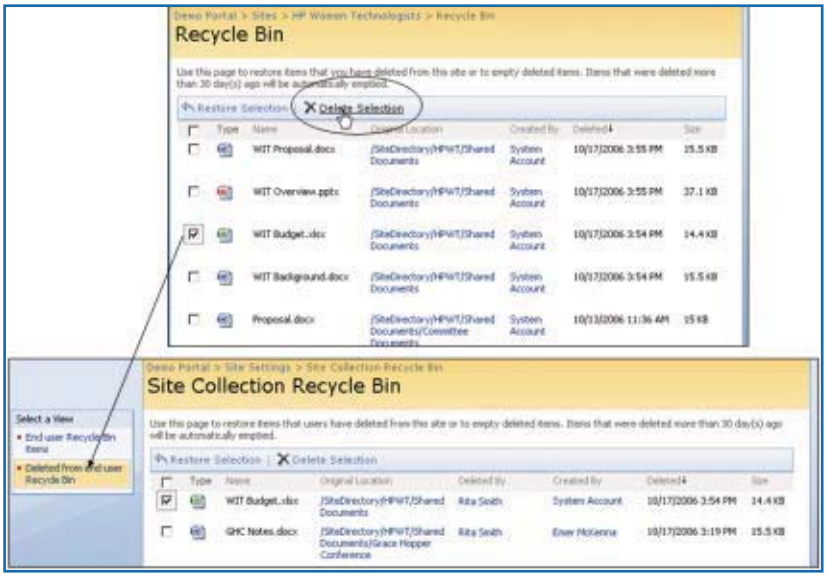


Figure 2: *WSS 3.0 two-stage Recycle Bin*

InstantDoc ID 96139

Emer McKenna
(emer.mckenna@hp.com) is a senior technology consultant in the HP Services Advanced Technology Group. She is the coauthor of *Microsoft SharePoint Technologies: Planning, Design and Implementation* (Digital Press).

What's Hot This Summer:

Technical Topics You Can't Afford to Miss

Now's the time to settle into some sizzling summer reading on the latest IT trends and technologies. These eBooks offer an in-depth look into topics such as email security, disaster recovery, messaging management, emerging technologies and more. View a complete listing of eBooks at windowsitpro.com/ebooks.

File Area Networks: Your First Look at FAN Technology

Gain control over the growing amount of file data in your enterprise. Learn how File Area Networks (FANs) can help you centralize file consolidation, migration, replication, and failover. Start streamlining your file management projects today!
windowsitpro.com/go/brocade/julyad

Data Protection and Disaster Recovery Tips

Discover a wealth of information about how to protect and secure your data in the event of a disaster. You may not be able to predict the exact details of a disaster, but you can be prepared with a solid response for when one strikes. Disaster can strike anywhere—not just where severe weather can hit—so make sure you're ready when it does.
windowsitpro.com/go/ca/julyad

Messaging Management

A secure mail and messaging infrastructure is fundamental to your business and any organization should plan for the appropriate message hygiene, availability, and control services from the start. Introduce yourself to three fundamental mail and messaging management services—security, availability and control services—and learn how to implement them.
windowsitpro.com/go/symantec/julyad

Spam Fighting and Email Security for the 21st Century

Protect your users and your network against email-borne threats. Gain the knowledge required to understand the real threat that email-borne attacks pose, and how to address those attacks in a way that reduces risk while ensuring users aren't impacted.
windowsitpro.com/go/ironport/julyad

Windows IT Pro SQL Server magazine

At a Glance

Q: What is Windows DreamScene, and how does it affect my computer's performance?

A: One of the attractions of Windows Vista Ultimate Edition is its Ultimate Extras that are made available via Microsoft Update. These Ultimate Extras offer additional functionality, such as improvements to BitLocker Drive Encryption, a poker game, and DreamScene, which lets you configure a video (.mpeg or .wmv format) to be used as your desktop background instead of a static picture, provided your computer has the power to handle the Windows Aero UI. The list of Ultimate Extras is available at http://windowsultimate.com/Blogs/Extras/Default.aspx and will grow as Microsoft develops more "extras." The programs are available via Microsoft Update or the Windows Ultimate Extras section of the Vista Welcome Center.

If you install DreamScene and choose to use a video as the desktop background, the amount of CPU and memory utilization will vary according to the video selected. When I used a video as my desktop background, the Windows Explorer process showed about 15 percent more CPU usage on a dual-core AMD 4400+ processor and showed that it used 50MB of memory. Although the amount of memory that the feature uses isn't a big problem, the processor hit might slow down certain functions. WMV files use heavy compression and therefore use more CPU than MPEG files use, so consider that when selecting a video. You also need to consider hardware because graphical processing units on some machines can take over the MPEG processing, and therefore the machine uses less CPU. You can also download a DreamScene add-on from http://dream.wincustomize.com that gives you access to many .dream files that you can use on your machine.

InstantDoc ID 96101

—John Savill

Q: When I try to install Adobe Acrobat Reader 8 on a machine running Windows Vista, I get the error message "The Temp folder is on a drive that is full or is inaccessible. Free up space on the drive or verify that you have write permission on the Temp folder." What's the problem?

A: This error message probably means you have User Account Control (UAC) disabled, which interferes with something in Acrobat's setup routine. To work around the error, right-click the AdbeRdr80_en_US.exe file, select Properties, and navigate to the Compatibility tab. Select the option to run in compatibility mode and select Windows XP (Service Pack 2), as Figure 1 shows. The installation will now proceed without error.

InstantDoc ID 96102

—John Savill

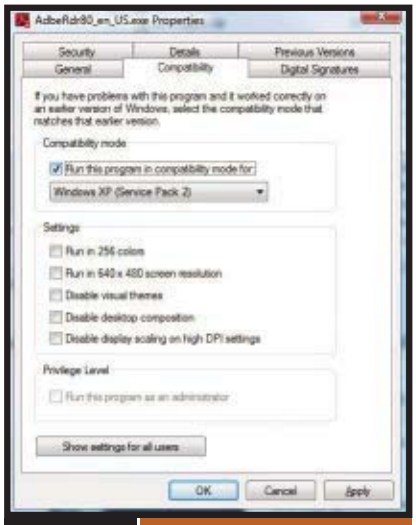


Figure 1: Working around an Acrobat compatibility problem

Q: I've been experimenting with using the command line, and I wonder if you could recommend an easy way to run a certain command depending on whether another command succeeds or fails?

A: Three methods exist for running commands together at the command prompt, a procedure known as chaining commands. The simplest method is to use a single ampersand (&) symbol, which simply runs multiple commands consecutively. For example,

```
command1 & command2
```

Command1 runs first, followed by command2, regardless of the success of command1. For example, running

```
dir & echo %time%
```

will list a folder, then write the current time. You aren't limited to two commands; you can keep adding commands, with each command separated by an ampersand.

If you require a second command to run only if the first command succeeds, you can use two ampersand (&&) characters. For example, if you run Setx with an invalid argument, the second command won't run:

```
C:\>setx /goobledegook && echo
  worked ERROR: Invalid syntax.
```

Whereas when I use a valid command, the second command runs and produces the following output:

```
C:\>setx var2 work && echo
worked
SUCCESS: Specified value was
saved. worked
```

You can use a double pipe || to run a command only if the previous command fails, as this example shows:

```
C:\>setx /goobledegook || echo
not working
ERROR: Invalid syntax.
 not working
```

InstantDoc ID 96103

—John Savill

John Savill
(jsavill@windowsitpro.com)

Ask the Windows IT Pro Community

For answers to more of your Windows Server 2003, Windows XP, Windows 2000, and Windows NT questions, visit our online discussion forums at http://www.windowsitpro.com/forums.

Chml Fills the Gap

A homemade tool makes Icacls even more useful

In last month's column, "Icacls Shows Integrity" (InstantDoc ID 95681), I used Windows Vista's new Icacls command-line tool to experiment with *integrity levels*—the new-to-Vista security notion of assigning labels to processes, users, and objects (e.g., files, folders, registry keys). This time, I want to address an Icacls shortcoming by sharing a free tool with you. My Chml file lets you take your integrity-level experiments to new areas of functionality.

A Short Review

Last month, I explained that Vista uses five integrity levels—Untrusted, Low, Medium, High, and System—to indicate an object's degree of trustworthiness. Administrators get a High integrity level, and non-administrative users get a Medium integrity level. By default, Windows enforces a *no write up* policy, which means that when a process tries to modify an object, Windows checks the integrity levels of the process and the object. If the process is running at a lower integrity level than the object, Windows blocks the modification attempt—even if the user has a Full Control permission on that object.

Icacls lets you modify integrity levels between Low, Medium, and High, but it won't let you do anything involving Untrusted or System levels, and it won't let you change the default *no write up* policy. That's a shame, because Windows can also enforce a *no read up* policy, which blocks any low-integrity process from *reading* the object. Having the ability to change the *no write up* policy to *no read up* could by quite useful: Wouldn't it be nice to add a little protection to personal files by setting them to a High integrity level with a *no read up* policy? Because most applications run at a Medium integrity level, such a setting would foil any spyware attempting to peek at, for example, a file containing your passwords or credit card information.

A Free Tool

I wanted to explore *no read up* policies and experiment with Untrusted and System integrity levels, so I wrote a tool that I call Chml, which you can find at my Web site (http://www.minasi.com/vista/chml.htm). Download the chml.exe file, and copy it to your \Windows\System32 folder so that it will be on your system path and thus always accessible from a command prompt. Then, ensure that you have the *Modify an object label* user privilege that I discussed last month. Open an elevated command prompt, change to the C:\stuff folder that you created last month, and you're ready to start running Chml.

Create a text file of some kind, and call it *test1.txt*. Now, you've got something to work with. Ask Chml to tell you the file's current integrity level by typing

```
chml test1.txt
```

and it will inform you that the file is unlabeled, but that *unlabeled* means the OS treats it as having a Medium integrity level. Now, raise the file's integrity level to High by typing

```
chml test1.txt -i:h
```

The -i: option can take the values *u, l, m, h,* or *s*, and these values are case-sensitive (as are all Chml options). Chml will confirm that it has successfully set test1.txt's integrity level to High. If you type

```
icacls tes1t.txt
```

Icacls will confirm that the file has a label of Mandatory Label\High Mandatory Level, which—as you learned last month—is Vista's way of saying that a file has a High integrity level.

Now, give test1.txt a *no read up* policy by typing

```
chml test1.txt -i:h -nr
```

You can use any combination of the -nr, -nw, and -nx options to assign the *no read up, no write up,* or *no execute up* policies. (I haven't come up with any uses for the *no execute up* policy.)

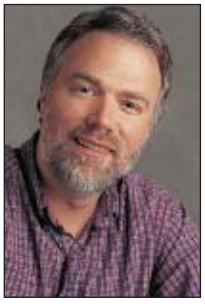
Running Icacls on test1.txt will show a different label than before: Mandatory Label\High Mandatory Level:(NR). This label is different from the labels you've seen before because previous labels have ended with (NW). As you've probably guessed, NW means a *no write up* policy, and NR means a *no read up* policy.

Now open a non-elevated command prompt and try to examine test1.txt by typing

```
type test1.txt
```

You'll get an Access Denied error message, despite the fact that you're the owner of the object. That's *no read up* in action. But that's not all that Chml can do, as you'll see next month.

InstantDoc ID 95973



Mark Minasi (http://www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 25 books, including *Administering Windows Vista Security: The Big Surprises* (Sybex). He writes and speaks around the world about Windows networking.

Did You Know?

Learn more about Icacls in our Security Pro VIP article "Icacls," http://www.securityprovip.com, InstantDoc ID 95657.

Vista Customizations for Administrators

Make Vista look and perform the way you want it to

Michael Otey
(mikeo@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and coauthor of *SQL Server 2005 Developer's Guide* (Osborne/McGraw-Hill).

If you've ever watched a baseball game, you've probably noticed that the batter starts shuffling the dirt at his feet as soon he steps into the batter's box, scraping and pushing till it feels just right so he can focus on the work at hand: hitting the ball. For the IT administrator who's used to working with Windows XP, moving to Windows Vista might take the same kind of adjustment. Here are 10 ways you can customize Vista for use as an administrative desktop to help you get your job done.

10 Add your picture to the Welcome screen—If you get tired of appearing as a red flower, you might want to personalize the picture Vista uses for the Welcome screen and the Start menu. To customize your picture, open Control Panel, click User Accounts and Family Safety, then click *Change your picture* followed by *Browse for more pictures* to navigate to a saved photo.

9 Display file extensions—I'm a Windows Explorer–centric user, so customizing Windows Explorer is my first piece of business with any new OS. I can't work effectively if I can't see file extensions with file names. To show file extensions in Vista, open Windows Explorer and click Folder and Search Options on the Organize menu. Click the View tab and clear the *Hide file extensions for known file types* check box.

8 Show hidden files—While you've got the Folder and Search Options dialog box open, the next customization you might want to make is to display hidden files. Scroll through the Advanced settings and select *Show hidden files and folders*.

7 Show system files—The other important Windows Explorer option that you'll probably want to enable for administrative desktops is to show system files. Scroll through the Advanced settings on the Folder and Search Options dialog box and clear the *Hide protected operating system files* check box.

6 Put the Run command on the Start menu—One casualty in Vista's UI is the Run command. With XP and Windows 2000, the Run command is on the Start menu, but in Vista it's buried under All Programs, Accessories. To put the Run command back on the Start menu, right-click the Start button, choose Properties, then click Customize. Scroll through the list and select *Run command*, then click OK.

5 Enable File Sharing—Because I synchronize files with my laptop and access my system from other machines on the network, I like to have file sharing enabled. By default, Vista's file sharing is turned off. To enable file sharing, click Start, Control Panel, Network and Internet, and open the Network and Sharing Center. In the Sharing and Discovery section, click *File sharing*, then select *Turn on file sharing*.

4 Use Open Command Window Here—Open Command Window Here was my favorite PowerToys add-on to XP. With Vista, it's included as a part of the OS, but how to use it isn't exactly obvious. To use Vista's Open Command Window Here function, hold down the Shift key and right-click a folder name in Windows Explorer. This function works only in the right-hand Windows Explorer pane.

3 Show Network Connections on the desktop—Vista's Network Connections folder can be found through the Network and Sharing Center by clicking *Manage network connections*. To add the Network Connections window directly to the desktop, right-click the desktop and choose New, Shortcut. Enter ncpa.cpl, then click Next. Name the shortcut Network Connections, then click Finish.

2 Show the Computer icon on the desktop—The old My Computer icon on the desktop was a UI feature I found pretty handy in previous versions of Windows. To display the new Computer icon on the Vista desktop, click the Start button, then right-click the Computer option and choose Show on Desktop from the pop-up menu.

1 Enable Aero Glass—After upgrading your system to be Aero Glass–capable, you might be surprised to find that the Aero Glass interface isn't being displayed. To get your upgraded system to display the cool new interface, right-click the desktop and select Personalize. Then click Window Color and Appearance. Select Windows Aero from the *Color scheme* drop-down menu, then click Apply.

InstantDoc ID 96011

HOW WELL ARE YOUR SERVERS PROTECTED?

When it comes to disaster, it's not IF, but WHEN. And too often, it's when you least expect it.

Get High-Availabilty and Disaster Recovery "In-One" With Double-Take®. It is your job to keep servers up, data available and prevent downtime. Failure to protect mission critical data and applications can set your business back by weeks, months or worse. Disaster recovery is now one of the highest IT priorities.

In today's business climate, you have to have a tested plan and reliable tools in place for the moment your server (or site) goes down. Double-Take is that tool. Sold more than all other High-Availability tools combined, it is even certified for W2K Datacenter. No other HA tool is. A whole department sitting on their hands can cost thousands of dollars per minute. The ROI of Double-Take is a no-brainer.

Double-Take delivers real-time data replication combined with fail-over so you have high-availability and disaster recovery for your (virtual) Windows Servers -- safely and securely. This is the reason that hundreds of Fortune 500 companies worldwide use Double-Take to ensure their business continuity. Three levels of data compression allow more data to be replicated and increase performance and scalability.

Double-Take®

Double-Take gives you the peace of mind your data is safe and your job secure. Don't wait. *Download a free 30-day eval copy right now* and start protecting your data and applications.

Certified for Microsoft® Windows Server™ 2003 Standard Edition Enterprise Edition Datacenter Edition

Download your free eval copy today!

Sunbelt Software

Sunbelt Software Tel: 1-888-688-8457 or 1-727-562-0101 Fax: 1-727-562-5199 www.sunbelt-software.com sales@sunbelt-software.com

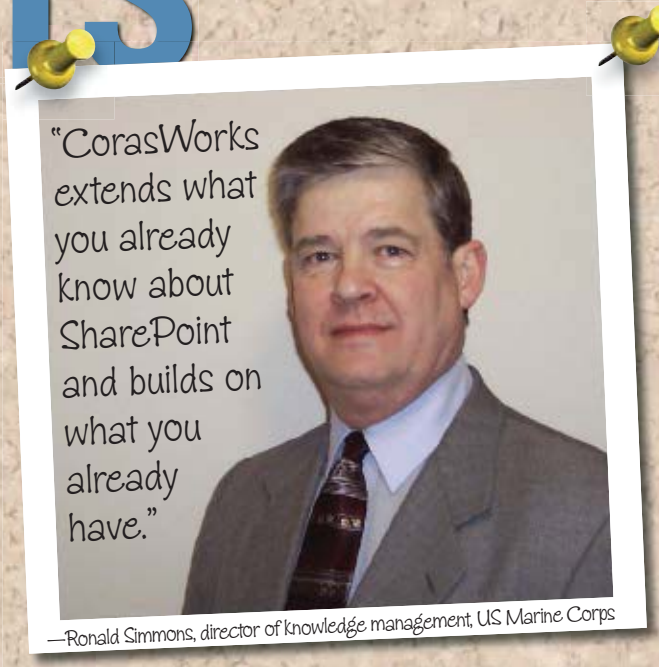
Blake Eno (beno@windowsitpro.com)
is product editor for *Windows IT Pro* and *SQL Server Magazine*.

At a Glance

Readers Review HOT PRODUCTS

Build Applications on SharePoint

CorasWorks Workplace Suite



—Ronald Simmons, director of knowledge management, US Marine Corps

In my work with the US Marine Corps (USMC), I was involved in reevaluating day-to-day business processes and methods of collaboratiom. We came to the realization that the USMC collaborated and performed day-to-day business processes using just email. We decided to move the USMC's business processes from email to **CorasWorks** Workplace Suite so we could more easily manage projects, automate processes, and create custom solutions.

Workplace Suite completely changed how the Marines do business and empowered us to modernize our business processes. For example, the Marines have a program called the Urgent Universal Needs System (UUNS), which is the process Marines in the field use when they desperately need a piece of equipment they don't have in order to accomplish their mission. Before CorasWorks Workplace Suite, the UUNS approval process consisted simply of a Microsoft Word document attached to an email message. Using CorasWorks, we moved data onto SharePoint, and Workplace Suite's charting capabilities let us track the number and status of UUNS requests. CorasWorks also lets Marines push email messages to the appropriate people.

I like solutions built for people who have average skill sets—I avoid products that require extensive IT knowledge and expertise. CorasWorks has the same philosophy, and Workplace Suite lets us create our own solutions on top of SharePoint even though we're not IT gurus. CorasWorks extends what you already know about SharePoint and builds on what you already have.

Reader: Ronald Simmons Director of knowledge management, US Marine Corps
Product: CorasWorks Workplace Suite
Company: CorasWorks
Contact: www.corasworks.net, 703-797-1881 or 866-580-3115

What's Hot continues on page 76

Wanted: Your Real-World Experiences with Products

Have you discovered a great product that saves you time and money? Do you use something you wouldn't wish on anyone? Tell the world in a review right here in What's Hot: Readers Review Hot Products. If we publish your opinion, we'll send you a Best Buy gift card! Send information about a product you use and whether it helps you or hinders you to whatshot@windowsitpro.com.

The Best Choice For Yo

Save 50 %

Limited Time Offer!

Click-n-Build

Hassle-free hosted applications. APS certified.

APS Gold Provider

Improve your website - with just the click of a mouse! Click-n-Build is an APS (Application Packaging Standard) certified solution that helps you build and improve your website with a variety of software applications. These hassle-free applications are accessible directly through your 1&1 Control Panel. We manage the installation process, updates and security patches for you. Now FREE with our Linux Business Package!

MEMBER OF united internet

Call **1.877.go1and1**

ur Website!

Exclusive Limited Time Offers
Visit our website today!

	1&1 BUSINESS	Yahoo! STANDARD	Go Daddy PREMIUM
Included Domains	3	1	$1.99/year with purchase
Web Space	250 GB	10 GB	200 GB
Monthly Transfer Volume	2,500 GB	400 GB	2,000 GB
E-mail Accounts	2,500 IMAP or POP3	500 POP3	2,000 POP3
Mailbox Size	2 GB	2 GB	10 MB
Search Engine Submission	✓	✓	Extra charge applies
Website Builder	18 Pages	✓	Freeware
Flash Site Builder	18 Pages	–	–
Photo Gallery	✓	✓	✓
RSS Feed Creator	✓	–	$4.99/month
Ad-free Blog	✓	✓	Freeware
Map & Driving Directions	✓	✓	–
Dynamic Web Content	✓	✓	–
Web Statistics	✓	✓	✓
E-mail Newsletter Tool	✓	$10/month	$3.99/month
In2site Live Dialogue	✓	–	–
Chat Channels	✓	–	✓
Form Builder	✓	✓	–
Click-n-Build Applications	5	–	–
Premium Software Suite	✓	–	–
90-Day Money Back Guarantee	✓	–	–
Support	24/7 Toll-free Phone, E-mail	24/7 Toll-free Phone, E-mail	24/7 Phone, E-mail
Price Per Month	**$9.99**	**$19.95**	**$14.99**
SPECIAL OFFER	**50% off first 3 months!***	–	–
TOTAL/YEAR	**$104.90**	**$239.40**	**$179.88**

We offer a variety of hosting packages to fit your needs and budget.

DOMAINS

.info

Give your site international appeal!
Reach a worldwide audience with the universally recognized .info domain.

$2.99 per year

SERVERS

Save up to **$177**

Need more power?
Our Virtual Private Server meets the gap between high-end web hosting and dedicated servers.

3 months FREE!

PayPal™
Now accepting PayPal™

1&1

Visit us now **1and1.com**

Learn to Solve AD Problems

O'Reilly Media's *Active Directory Cookbook*

Many of the books on Windows Server 2003 and Active Directory (AD) are very good, but Robbie Allen's *Active Directory Cookbook* (from **O'Reilly Media**) is the best book I've ever read. The book has many "recipes"—procedures for doing certain AD tasks—using commands fired from the command prompt, Visual Basic (VB) scripts, or a GUI console.

Reader:
Murat Yildirimoglu
MCSE, MCT

Product:
Active Directory Cookbook

Company:
O'Reilly Media

Contact:
www.oreilly.com,
707-827-7000 or
800-998-9938

There's also a lot of invaluable information about the architecture of AD. For example, I learned why the password and account lockout policies are domain-wide: They are attributes of the domain object (domain class). I also learned how to easily increase the AD quota that limits the number of machine accounts end-users can add. The quota information resides on the domain object in the ms-DS-MachineAccountQuota attribute, which has a default value of 10, but you can change that value to whatever value you like by using the Microsoft Management Console (MMC) ADSIEdit.msc snap-in. Other invaluable information I learned was how to move computer accounts from one container to another by using the Active Directory Users and Computers snap-in, the Dsmove command, or a VB script. What differentiates this book is the under-the-hood information in it and the alternative methods it provides for accomplishing AD tasks.

> "Active Directory Cookbook is the best book I've ever read."
>
> —Murat Yildirimoglu, MCSE, MCT

What's Hot continues on page 77

Put Security at the Heart of the Network

High Tower Software's High Tower SEM 3210

Reader:
Glenn Haar
Enterprise security coordinator
Product:
High Tower SEM 3210
Company:
High Tower Software
Contact:
www.high-tower.com,
949-330-3080 or
877-448-6937

As the enterprise security coordinator for the Idaho Tax Commission, I led our security team on a major project to replace the entire infrastructure of our network. Because we were responsible for complying not only with state requirements but also with Internal Revenue Service requirements, it was essential that security be at the heart of the network. We needed a security event management (SEM) solution that could collect, correlate, and analyze data from all devices in our network. Also very important to us was minimizing the amount of time spent managing the solution so we could put our existing human resources to better use.

We purchased **High Tower Software**'s High Tower SEM 3210 appliance and put it at the center of our new network. The appliance correlates and analyzes data from devices around the network, alerting us to potential problems and letting us target our resources at legitimate concerns instead of spending time reviewing tons of data manually. What helped separate High Tower Software from the competition was its uncomplicated licensing scheme (some vendors require a license for every host that you collect data from) and its overall understanding of security and our unique requirements.

> "What helped separate High Tower Software from the competition was its uncomplicated licensing scheme."
>
> Glenn Haar, enterprise security coordinator

InstantDoc ID 96278

DIRECTORY OF SERVICES

Windows IT Pro Network

Search our network of sites dedicated to hands-on technical information for IT professionals.

http://www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.

http://www.windowsitpro.com/forums

News

Check out the current news and information about Microsoft Windows technologies.

http://www.wininformant.com

EMAIL NEWSLETTERS

Get free NT/2000/XP/2003 news, commentary, and tips delivered automatically to your desktop.

- *Windows IT Pro UPDATE*
- *Vista UPDATE*
- *Windows Tips & Tricks UPDATE*
- *WinInfo Daily UPDATE*
- *.NET Briefing*
- *Exchange & Outlook UPDATE*
- *Scripting Central*
- *Security UPDATE*
- *SQL Server 2005 Express UPDATE*
- *SQL Server Magazine UPDATE*
- *Storage UPDATE*
- *Windows IT Library UPDATE*
- *Connected Home EXPRESS*

http://www.windowsitpro.com/email

PRO VIP ACCESS

Exchange & Outlook Pro VIP

Discover smart solutions for Exchange and Outlook administrators.

http://www.exchangeprovip.com

Scripting Pro VIP

Learn how to create more powerful scripts and get tips for automating those tedious administrative tasks.

http://www.scriptingprovip.com

Security Pro VIP

Discover practical, how-to advice for avoiding and solving security problems.

http://www.securityprovip.com

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles. Contact Joel Kirk at jkirk@penton.com.

Super CD/VIP

Get exclusive access to all of our print publications, including *Windows IT Pro,* via the new, banner-free VIP Web site.

http://www.windowsitpro.com/sub/vip

Article Archive CD

Access every article ever printed in *Windows IT Pro* magazine since September 1995 with this portable and speedy tool.

http://www.windowsitpro.com/sub/cd

SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.

http://www.sqlmag.com

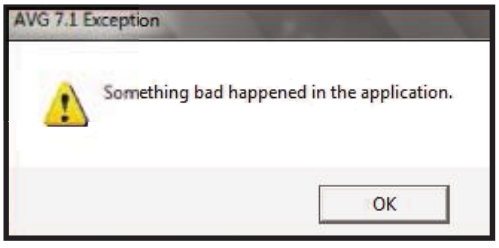
For detailed information about products in this issue of *Windows IT Pro*, visit the Web sites listed below.

VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

Send your funny screen shots, juicy rumors, or industry humor to rumors@windowsitpro.com. If we use your submission, you'll receive a Ctrl+Alt+Del coffee mug.

UNFORTUNATE WAYS TO START YOUR MORNING



I'm afraid to ask...

Just clean up the mess, OK?

Ah, that's better.

You seem to lack confidence in your judgment.

DILBERT® by Scott Adams

July 2007 issue no. 155, *Windows IT Pro* (ISSN 1552-3136) is published monthly. Subscriptions in US, $49.95 for one year; in Canada, $59 US currency, plus 7% for GST for one year; in UK £59; in all other countries, US $99. *Windows IT Pro,* 221 E. 29th St., Loveland, CO 80538, (800) 793-5697 or (970) 203-2782. Sales and Marketing Offices: 221 E. 29th St., Loveland, CO 80538. Advertising rates furnished upon request. Periodicals Class postage paid at Loveland, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,* P.O. Box 447, Loveland, CO 80539-0447. SUBSCRIBERS:** Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, P.O. Box 447, Loveland, CO 80539-0447. Printed in the USA. BPA Worldwide Membership Applied for May 2006.

"Raise your hand if you are a domain admin"

LESSON #1: DELEGATE SECURELY WITH ACTIVE ADMINISTRATOR.

Overprivileged users and other security risks in your Active Directory can be a major threat to your AD infrastructure. Active Administrator™ is an enterprise-class Active Directory management and auditing solution that won't land you in AD-detention:

SIMPLIFIED SECURITY WITH ACTIVE TEMPLATES

Take the guesswork out of delegation and ensure consistent assignment of permissions.

SELF-HEALING AD SECURITY TEMPLATES

Automatically recreate broken or missing permissions.

POWERFUL ACTIVE DIRECTORY AUDITING

Centrally audit the changes made to AD objects and Group Policy, without sifting through thousands of event log entries.

To download a free 30-day evaluation, visit
www.scriptlogic.com/ADSchool

SCRIPTLOGIC®

Point, Click, Done!